English

openFT V12.0 for BS2000/OSD

Installation and Administration

System Administrator Guide

Edition September 2012

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to:
manuals@ts.fujitsu.com

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Contents

1 Introduction

The openFT product range transfers and manages files

– automatically,
– securely, and
– cost-effectively.

The reliable and user-friendly transfer of files is an important function in a high-performance computer network. The corporate topologies consist of networked PC workstations, which are usually additionally linked to a mainframe or Unix based server or Windows server. This allows much of the processing power to be provided directly at the workstation, while file transfer moves the data to the mainframe for further processing there as required. In such landscapes, the locations of the individual systems may be quite far apart. Fujitsu Technology Solutions offers an extensive range of file transfer products - the openFT product range - for the following system platforms:

- BS2000/OSD“
- Solaris^{TM} (SPARC“/Intel^{TM}), LINUX“, AIX“, HP-UX“
- Microsoft“ Windows Vista^{TM}, Windows^{TM} 7, Windows Server 2008^{TM} and Windows Server 2008 R2^{TM}
- z/OS (IBM“)

1.1 Brief description of the product openFT for BS2000/OSD

openFT for BS2000/OSD is the file transfer product for computers using the operating system BS2000/OSD.

All openFT products communicate with each other using the openFT protocol (previously known as FTNEA) as laid down by Fujitsu. Since a number of FT products from other software suppliers also support these protocols, many interconnection options are available.

openFT allows the use of TCP/IP, ISO TP0/2, ISO TP4, SNA and NEA as transport protocols.

The range of functions made available by openFT can be extended using the add-on products openFT-FTAM, openFT-FTP and openFT-AC:

- openFT-FTAM supports the FTAM file transfer protocol (File Transfer Access and Management) standardized by ISO (International Organization for Standardization). This makes it possible to interconnect to systems of other manufacturers whose FT products also support the same standard.
- openFT-FTP supports FTP functionality
- openFT-AC provides extended system and data access protection. FTAC stands for File Transfer Access Control.

1.2 Target group and objectives of this manual

This manual is intended for FT administrators and FTAC administrators.

To understand this manual, it is necessary to have a knowledge of the BS2000/OSD operating system.

1.3 Concept of openFT for BS2000/OSD manuals

The complete description of openFT and its optional components openFT-FTAM for BS2000, openFT-FTP for BS2000 and openFT-AC for BS2000 is contained in four manuals. In addition to this System Administrator Guide, there is also a User Guide, a Programmer Reference Guide and a Message Manual. The description is divided between the four manuals as follows:

- openFT for BS2000 - Installation and Administration

  The System Administrator Guide is intended for FT and FTAC administrators. It describes:
  - the installation of openFT and its optional components
  - operation, control and monitoring of the FT system and the FTAC environment
  - the administration commands for FT and FTAC administrators
  - account records

- openFT for BS2000 - Managed File Transfer in the Open World

  The User Guide contains the following information:
  - an overview of the basic functions of the openFT product family
  - a detailed description of the conventions for the file transfer to computers with different operating systems
  - information on the implementation of FTAM
  - description of the user commands
  - messages from openFT and openFT-AC

- openFT for BS2000 - Programming Interfaces

  The Programmer Reference Guide describes the openFT and openFT-AC program interfaces.

If openFT for BS2000/OSD is included in remote administration by means of a remote administration server, you can find information on configuring a remote administration server in the following manuals:

- “openFT V12.0 for Unix Systems - Installation and Administration” or
- “openFT V12.0 for Windows Systems - Installation and Administration”

You will also find current information on the Internet under *http://de.ts.fujitsu.com/openft* (german) or *http://ts.fujitsu.com/openft* (english).

1.4 Organization of the System Administrator Guide

This System Administrator Guide describes the command interface and tools available to FT and FTAC administrators. It is divided into six chapters.

This first chapter describes the layout of this manual and the changes introduced in openFT V12.0 for BS2000 as compared to the previous version V11.0.

The second chapter describes the installation of openFT for BS2000 and the prerequisites for using this product.

The third chapter describes the operation, control and monitoring of openFT and openFT-AC. It discusses the logging function, the SNMP connection, how to optimize the operating parameters, and what to do in the event of errors.

Remote administration and the associated interfaces of openFT for BS2000/OSD are introduced briefly in the fourth chapter.

The fifth chapter describes the administration commands that are used by the FT/FT-AC administrator as tools in discharging his or her administrative duties.

The appendix contains a description of the command output in CSV format, an explanation of the FT accounting records. and the openFT console messages.

1.5 Changes since the last version of the manual

The following changes have been introduced in the openFT V12.0 for BS2000/OSD System Administrator Guide since the earlier version openFT V11.0 for BS2000/OSD:

Extended logging functions

The logging functions have been extended as follows:

- Switch log file and offline logging

  The log file can be changed during operation. After switchover, new log records are written to a new log file. The previous log file is retained as an offline log file. The log records it contains can still be viewed using the tools available in openFT.

  To permit this, the command interface has been extended as follows:

  – MODIFY-FT-OPTIONS:

    New operand value LOGGING=*CHANGE-FILES to switch the log file.

  – SHOW-FT-LOGGING-RECORDS:

    New operands LOGGING-FILE and PREVIOUS-FILES that make it possible to view log records from offline log records.

    New operand value INFORMATION=*LOGGING-FILES to output the names of all log files (including offline log files).

  – DELETE-FT-LOGGING-RECORDS:

    New selection criterion *LOGGING-FILES to delete offline log files.

- Automatic deletion of log records

  Intervals for the automatic deletion of log records can be set in the operating parameters. To make this possible, the MODIFY-FT-OPTIONS command has been extended by the new operand DELETE-LOGGING. The settings can be displayed using the SHOW-FT-OPTIONS command.

- Polling function for the output of log records

  In SHOW-FT-LOGGING-RECORDS, the new operand NUMBER=*POLLING can be used to set the interval and number of repetitions (polling).

- Wildcards for partner names during the output of log records

  In SHOW-FT-LOGGING-RECORDS, it is also possible to use the wildcards "*" and "?" when specifying the partner name.

Enhanced security functions

- Import keys

  The new command IMPORT-FT-KEY can be used to import both externally generated private keys and the public keys of partner systems.

- Expiration data and authentication level of RSA keys

  – Using the new command MODIFY-FT-KEY, it is possible to define an expiration date and modify the authentication level (1 or 2) for keys that are used for the authentication of partner systems.

    > ℹ Authentication level 2 was introduced with openFT V11.0B and meets higher security requirements.

  – The new command SHOW-FT-KEY can be used to output the attributes of the keys stored in the system.

  – SHOW-FT-LOGGING-RECORDS displays the authentication level (output parameter SEC-OPTS, new values LAUTH2 and RAUTH2).

- Force data encryption

  The new operand ENCRYPTION-MANDATORY in the MODIFY-FT-OPTIONS command can be used to force data encryption for file transfer and administration requests. The settings can be made separately for inbound and outbound requests.

- Following installation, openFT uses an RSA key of length 2048 by default.

Extended partner management

- Partners in the partner list can also be explicitly deactivated for inbound requests.

  To permit this, the syntax of the STATE operand in the commands ADD-FT-PARTNER and MODIFY-FT-PARTNER has been modified and the parameters INBOUND and OUTBOUND have been added. In SHOW-FT-PARTNERS, the current setting is displayed in the output parameter INBND.

  > ℹ The syntax previously used for STATE is still valid provided that the new functions are not used.

- Serialization of asynchronous outbound requests to a specific partner

  The new operand REQUEST-PROCESSING in the commands ADD-FT-PARTNER and MODIFY-FT-PARTNER makes it possible to control whether asynchronous outbound requests to a specific partner should always be run serially or whether parallel connections are also permitted. In SHOW-FT-PARTNERS, this attribute is displayed in the output parameter REQU-P.

Extended request management

- Global request ID

  In the event of an FT request, the initiator's request number is transferred to the responder where it is visible as a global request ID. This means that any request can be unambiguously assigned to an initiator and responder.

  The SHOW-FILE-TRANSFER and SHOW-FT-LOGGING-RECORDS commands have been extended as follows:

  - At the responder, the global request ID is displayed in the new output parameter GLOB-ID in each command.
  - The new parameter GLOBAL-REQUEST-ID makes it possible to perform selection on the basis of a global request ID in both commands.

- Display of canceled requests

  The new operand value STATE=*CANCELLED in the SHOW-FILE-TRANSFER command can be used to select canceled requests. This displays requests that have been canceled but not fully terminated. The output is available only to the FT administrator.

Other changes

- The maximum value for the TRANSFER-ID (request number) that can be specified in a number of different commands has been changed to 2147483647.
- In the commands CREATE-FT-PROFILE and MODIFY-FT-PROFILE, it is possible to specify the operand value ACCOUNT=*NONE for USER-ADMISSION and PROCESSING-ADMISSION. The user's default account number is then used.
- The description of the OPS variable in SHOW-FT-PARTNERS has been extended to include the parameters for ADM partners.
- The description of dynamic partners is now more precise. To this end, the partner types "named partner", "registered dynamic partner" and 'free dynamic partner" have been introduced.
- The description of the CSV output for the SHOW commands has been greatly extended.

1.6 Notational conventions

The following notational conventions are used throughout this manual:

ℹ indicates notes

⚠ Indicates warnings.

Additional conventions are used for the command descriptions, see section “Command syntax representation” on page 116.

1.7 README file

The functional changes to the current product version and revisions to this manual are described in the product-specific Readme file.

Readme files online

Readme files are available to you online in addition to the product manuals under the various products at *http://manuals.ts.fujitsu.com*.

Readme files under BS2000/OSD

On your BS2000 system you will find Readme files for the installed products under the file name:

```
SYSRME.OPENFT.120.E
SYSRME.OPENFT-FTAM.120.E
SYSRME.OPENFT-FTP.120.E
SYSRME.OPENFT-AC.120.E
```

Please refer to your system administrator for the user ID under which the required Readme file can be found. You can also obtain the path name of the Readme file directly by entering the following command:

```
/SHOW-INSTALLATION-PATH INSTALLATION-UNIT=<product>,LOGICAL-ID=SYSRME.E
```

You can view the Readme file on screen with `/SHOW-FILE` or by opening it in an editor, or print it on a standard printer using the following command:

```
/PRINT-DOCUMENT <filename>, LINE-SPACING=*BY-EBCDIC-CONTROL
```

Additional product information

Current information, version and hardware dependencies, and instructions for installing and using a product version are contained in the associated Release Notice. These Release Notices are available at *http://manuals.ts.fujitsu.com*.

2 Installation and startup

This chapter describes the actions and preconditions required to install and run openFT and any of the optional components openFT-FTAM, openFT-AC, openFT-FTP and openFT-CR in BS2000.

2.1 Installing openFT

openFT V12.0 requires the following software

– BS2000/OSD as of V7.0
– openNet server as of V3.2 (i.e. BCAM ≥ V19.0)

The following versions are required when using the optional add-on components:

– openFT-FTAM V12.0
– openFT-AC V12.0
– openFT-CR V12.0
– openFT-FTP V12.0

If you want to make use of the POSIX functionality, you will also need the BS2000/OSD component POSIX.

openFT-FTAM V12.0 requires:

– openFT ≥ V12.0
– OSS ≥ V4.1C

openFT-AC, openFT-FTP and openFT-CR V12.0 require:

– openFT ≥ V12.0

Delivery of openFT is done via the software delivery and information system SOLIS2. Installation is done via IMON. The installation routine incorporates the required BS2000-specific tasks such as the MSGFILE update, subsystem catalog entries and the integration of the SDF syntax file.

Whenever a program which uses FT interfaces is compiled, the file SYSLIB.OPENFT.120 for COBOL and ASSEMBLER programs must be available. This file must be available as a shareable file in the system, but need not be located under the TSOS ID.

2.1.1 Initial installation of openFT for BS2000/OSD

openFT is a subsystem and is not generated when the BS2000 system is generated.

The FT administrator commands can be issued from the console. Administration from the terminal requires the FT-ADMINISTRATION privilege, assigned by default to TSOS. If SECOS is in use, this privilege can be assigned to other user IDs. See the SECOS manual for details.

In order to ensure the usability of the COBOL program interface, the file SYSRTC.FT (runtime module for the COBOL program interface) must be shareable under the SYSFJAM ID (`SHARE=YES, ACCESS=READ`). COBOL programs produced with the COBOL interface load the runtime module from this ID.

The product PAMINT is used to convert from keyed to nonkey files (and vice versa). This product belongs to the BS2000 basic configuration and must be available under TSOS. PAMINT should be installed with IMON so that openFT can automatically load the current version and use it for conversion. If this is not possible, then openFT uses the file $TSOS.SYSLNK. PAMINT or $TSOS.SYSREP.PAMINT at link time. In this case, these files must therefore contain copies of the current PAMINT SYSLNK or SYSREP file.

2.1.2 Version change and compatibility

openFT V12.0 is compatible with openFT V11.0, i.e. all V11.0 functions can be used unchanged and without restriction in V12.0.

Change of version

Before performing installation with IMON, the following activities must be performed in all the instances present:

1. Back up the operating parameter settings, the partner list entries and, if applicable, the FTAC environment in procedure files, for details, see section “Backing up the configuration data” on page 97.
2. Back up the following openFT system files to the instance ID (default instance: $SYSFJAM) in case you should need to revert to the earlier version:

   SYSRQF
   SYSLOG
   SYSKPL
   SYSKEY
   SYSFSI

i Instead of backing up the SYSLOG as a file, you can, for example, simply back up the content of SYSLOG in CSV format and then evaluate the log records at a later date. To do this, use the command SHOW-FT-LOGGING-RECORDS LAYOUT=*CSV.
Following installation, openFT then works with a new SYSLOG file.

3. Make sure that there are no requests in the request queue when you perform the version change.
   Reason: Requests are not taken over from V11 to V12. As a result, unfinished requests are lost on migration and may even cause requests for which their is no correspondence in the local system to persist on partner systems.
4. Delete the files SYSOPF, SYSRQF and SYSPTF, and possibly also SYSLOG (if the old log records are no longer required in the new version). The SYSLOG file can only be taken over to V12 as an offline log file.
5. Leave the SYSKPL and SYSKEY files so that they can be taken over into the new version, if authentication is still to be used there. In this case, you must **not** delete these files!

After completion of the IMON installation of openFT (and possibly of openFT-FTAM or openFT-FTP), openFT recreates the files SYSRQF, SYSOPF and SYSPTF on the first access attempt.

Taking over settings

If you want to continue to work with the old operating parameter settings, partner list entries and, if applicable, FTAC settings, you should run the procedures generated during the backup operation (see point 1 on page 22).

Notes on openFT-FTP

When using openFT-FTP, you should note that after installation the FTP server is automatically deactivated.

If you want to use openFT-FTP for inbound requests, you have the following possibilities:

- You take over the operating parameter settings from openFT V11.0 provided that the openFTP server has been activated there.
- You activate the FTP server manually using the command MODIFY-FT-OPTIONS ...,ACTIVE-APPLICATIONS. When doing this, note the following:
  ACTIVE-APPLICATIONS=*ALL activates all protocols,
  ACTIVE-APPLICATIONS=*FTP only activates the FTP protocol.

For details, see section “MODIFY-FT-OPTIONS Modify operating parameters” on page 223.

2.1.3 Installation of the command interface for POSIX

openFT for BS2000/OSD supports the command interface which is provided in UNIX and Windows systems also in POSIX. This means that you can use the openFT functions in BS2000 from within a POSIX system. WIth a very few exceptions, the commands have the same function scope as they do in UNIX or Windows systems.

For details see the user guide and the administrator guide of openFT for UNIX Systems.

Installation

The library SINLIB.OPENFT.120 is required for installation. This contains the installation script and all the components needed for POSIX installation. The POSIX subsystem must be active for installation.

You install the command interface as follows:

- Call the START-POSIX-INSTALLATION command.
- Select “Install packages in POSIX” from the menu and enter the data in the “BS2000 POSIX package installation” screen which now opens. For details, see the POSIX manual “Basics for Users and System Administrators”.

2.2 Startup

The FT administrator's tasks have been simplified in openFT as of V10.0 since the request queue and partner list files are created when openFT is installed.

2.2.1 Preparing the FT system

ID and required PAM pages

For the first installation, an ID with the name SYSFJAM and the default catalog ID must be created for openFT on the home pubset of the processor. If you are running multiple openFT instances on your system, you must set up the configuration user IDs of the instances so that they are the same as SYSFJAM (the restriction concerning the home pubset does not apply here). The IDs should be set up in a manner that prevents a SET-LOGON-PARAMETERS command being entered. The number of PAM pages required by this ID depends on:

- the size of the request files and partner lists used and the required functionality, i.e., whether FTAC functionality is to be used. The openFT request queue SYSRQF has a default size of 12690 PAM pages while the option file SYSOPF requires 6 PAM pages and the partner list SYSPTF 1824 PAM pages. The FTAC file SYSFSA occupies at least 501 PAM pages.
- the size of the log file SYSLOG (at least 501 PAM pages) which, in turn, depends on the number of transfer requests handled and on which sets are engaged (i.e. only FT sets, only FTAC sets, or both).
- the size of the SYSFSI, SYSKPL, and SYSKEY files (by default, a total of 54 PAM pages), and on the number of key pairs (SYSPKF files) created.
- the type and number of trace functions activated.

It is therefore advisable to allow PAM page overruns for the ID SYSFJAM.

Access to public keys

In order to be able to access public keys, the FT administrator needs access to the SYSPKF files and the SYSKEY library on SYSFJAM or on the configuration user ID. If he/she does not have privileges granting him/her access to operating system resources, the FTAC admissions profiles should be set up to grant him/her access.

Starting and stopping the FT subsystem

openFT requires a subsystem catalog entry containing a subsystem declaration with the load time set to “AT-CREATION-REQUEST”. The FT subsystem must be explicitly loaded in a startup procedure (e.g. CMDFILE).

When an FT instance is stopped, (particularly by using /STOP-SUBSYSTEM FT) all the file locks held by openFT (see page 62) are cleared and, on loading an instance (e.g. by using /START-SUBSYSTEM FT), the locks are reset for files affected by existing requests. The FT or system administrator must therefore observe the following:

– On starting the FT subsystem, all pubsets that contain data that is to be used in the event of a restart must be available.
  On the other hand, the loading must also occur early enough to ensure that the files to be transmitted are protected in time. This also applies to the transfer files of all configured openFT instances.

– Unloading an FT instance should be done as late as possible, but before the export of the pubsets on which the files to be transmitted are located.

Result lists

The job class JBCLLST should be generated with a small maximum processing time and, if possible, a high selection priority for printing result lists. This job class should be accessible to all FT users. The high priority (JOBPRIORITY operand in job class setup) ensures that jobs of this type are quickly started. A low maximum processing time (CPU-TIME operand in job class setup) prevents these jobs blocking the processor for a prolonged time.

Follow-up processing

For follow-up processing initiated by the openFT, you should generate the job class JBCLJOB with low maximum processing time and, if necessary, a high selection priority. If you do not do this the default job class will be used for follow-up processing. You should start extended, CPU-intensive follow-up jobs as enter jobs using the job classes which are available as standard in the BS2000-System.

i Depending on the protocols configured, openFT can be reached via port 1100 (openFT protocol), 4800 (FTAM protocol), 21 (FTP protocol) and 11000 (FTADM protocol). To do this, openFT itself creates a BCMAP entry on START-FT. The following command is set for initializing mapping:

```
/BCMAP FUNCT=INIT,MAXMAP=500
```

If initialization is to be done using other values, it must take place before the first START-FT command.

2.2.2 Entering partners in the partner list

In openFT V10.0, the network description has been replaced by a partner list. The partner list is set up by openFT on installation. Following a new installation, it is empty.

Although the entry of partners in the partner list is optional, this offers significant advantages. These include simplified addressing for users, the central administration of partner addresses and enhanced security since you can assign individual properties such as security level or partner check level to partner systems, for example if authentication is required. Authentication requires partners to be entered in the partner list.

Consequently, you should enter partners with special characteristics in the partner list immediately after installation. The following options are available:

– If you are upgrading from an older openFT version, start the command procedure which you created with START-OPENFTPART or SHOW-FT-PARTNERS in the older openFT version. The previous entries are taken over into the partner list.

– ADD-FT-PARTNER command
This enters a new partner in the partner list.

In the operating parameters, you can specify that only the named partners from the partner list may be addressed (corresponds to the state up to openFT V9.0).

For further details on administering partners during operation, see section “Administering partners” on page 41.

2.2.3 Starting and stopping openFT

Starting openFT

openFT is started with the START-FT command. Care must also be taken to ensure that all pubsets are available, as otherwise any locally submitted request that requires an unavailable pubset will be terminated with an error message. If this happens, the user cannot be informed of the circumstances by an event list or a job variable.

START-FT starts all applications that have been activated using the command MODIFY-FT-OPTIONS .. ACTIVE-APPLICATIONS=.

If multiple instances are used on one computer, each instance must be started individually. Individual instances can be set up so that they are automatically started on executing the command START-SUBSYSTEM, see the section “Using openFT in a HIPLEX cluster” on page 88).

If the openFT option HOST-NAME is not set at start time then the real BCAM host is used. If multiple instances have to be started in a system then the host name must be set using the /MODIFY-FT-OPTIONS command at all but one of them.

Stopping openFT

Using STOP-FT terminates openFT in the current instance. When file transfer is terminated, non-restartable requests are aborted. Local requests continue to be accepted even after STOP-FT. The requests are stored in the request queue until openFT is restarted. When START-FT is entered again, the requests are processed in sequence.

2.3 Installing openFT-AC

The installation of openFT V12.0 is required for the installation of openFT-AC V12.0.

2.3.1 Initial installation

Delivery of openFT-AC takes place using the software delivery and information system SOLIS2. Installation takes place via IMON. If required, the installation contains BS2000-specific jobs such as MSGFILE update, subsystem catalog entries, and importing the SDF syntax file.

For the security of the SYSFSA file on the configuration user ID of the current openFT instance, it is recommended that you activate the class 2 ENCRYPTION option for password encryption. SYSFSA contains the settings for admissions sets and admissions profiles.

2.3.2 Version change

If an older version of openFT-AC is installed on your computer, it is recommended that you delete all product files of the old version with the exception of SYSFSA. Profiles and admission sets from the predecessor version V11 can be transferred unchanged.For all older versions, it is advisable to export the FTAC admission profiles and records using the EXPORT-FTAC-ENVIRONMENT command.

The openFT-AC system file SYSFSA (on all instance IDs) can be moved from V11 to V12. If it should become necessary to migrate back to the previous version, you should first back this file up or export it to an FTAC export file, because once SYSFSA has been opened by openFT V12, backward migration is no longer possible.

2.4 Configuring openFT-AC

Authorization of the FTAC administrator

It is recommended that the position of administrator for openFT-AC be given to a user in the system who is responsible for data protection in a BS2000 system, since he will know what protection measures are required where.

The FTAC administrator function is assigned by means of the SECOS privilege FTAC-ADMINISTRATION. It may also be assigned to several user IDs at once.
For BS2000 installations without SECOS, the administration attribute has a fixed assignment to the user ID TSOS.

FTAC administrators who possess both the FTAC administration and TSOS privilege have the following additional rights:

- If they import profiles (for any user ID), they can select whether the profiles will be immediately available and unrestricted, or whether they will be locked.
- If they create profiles for external IDs then these are also immediately available. This means that they can create valid transfer admissions even if they do not know the LOGON password of the target ID. This method can be used to set up profiles that remain valid after the LOGON password is modified.
- They can therefore also modify the transfer admissions of existing profiles with external IDs without knowing the profile owner’s password.

Adapting the default admission set

After the installation of openFT-AC, all values of the default admission set are set at 0!

This means that it is not yet possible to execute a file transfer with the local system. This is because as long as no other admission sets are made with MODIFY-FT-ADMISSION-SET, the default admission set is valid for all user IDs. The maximum security level 0 for the basic functions (inbound send, inbound receive, inbound follow-up processing, inbound file management, outbound send, outbound receive) means that these basic functions may not be used. The FTAC administrator must therefore use the command MODIFY-FT-ADMISSION-SET to raise the values of the default admission set.

Default security levels for partners

The FT administrator can use the MODIFY-FT-OPTIONS command (SECURITY-LEVEL operand) to define default security levels for all the partner systems entered in the partner list. The administrator can either enter a fixed value or specify *BY-PARTNER-ATTRIBUTES to indicate that the security level is set automatically: partners which are authenticated by openFT are assigned security level 10. Partners which are known in BCAM (i.e. they are addressed via their BCAM name) are assigned security level 90. All other partners are assigned security level 100.

This automatic assignment can also be activated on a partner-specific basis using the operands of the same name:
ADD-FT-PARTNER and MODIFY-FT-PARTNER...,SEC-LEV=*BY-PART-ATTR

This automatic assignment always applies to partners that are not in the partner list.

Examples

1. All partner systems should be accessible for file transfer for all FTAC users. This is achieved by setting all the values of the default admission set to100. The following command is used:

   ```
   /MOD-FT-AD␣*STD,MAX-LEV=100
   ```

   More information on the command MODIFY-FT-ADMISSION-SET can be found starting on page 213.

2. A differentiated setting of the default admission set might look as follows:

   ```
   /MODIFY-FT-ADMISSION-SET USER-IDENTIFICATION=*STD         -
                           MAX-LEVELS=(OUTBOUND-SEND=50,      -
                                       OUTBOUND-RECEIVE=50,   -
                                       INBOUND-SEND=20,       -
                                       INBOUND-RECEIVE=20,    -
                                       INBOUND-PROCESSING=10, -
                                       INBOUND-MANAGEMENT=0)
   ```

   The different security levels are assigned selectively. For example, the function “inbound management” can be fully blocked by setting the security level to 0.

   WARNING!

   Note that openFT-AC is only effective for connected products such as openFT or FTP. If other file transfer products without an openFT-AC connection are also being used, a more comprehensive and coordinated security concept would be advisable.

3 Operation of openFT

This chapter contains information on the subject of administration, security and control and monitoring functions.

FT and FTAC administration

An FT user can monitor and administer only his or her own FT requests, whereas the FT administrator has access to all FT activities occurring in his or her system.

The FTAC administration is independent of the FT administration. The FTAC administrator is the security manager of FT activities in your computer. He has “ultimate authority” over all admission sets and profiles.

If you also have SECOS in use, you will require the privilege FT-ADMINISTRATION for FT administration and FTAC-ADMINISTRATION for FTAC administration. In other cases, the system administrator ID TSOS must be used.

FTAC administrators who possess both the FTAC administration and TSOS privilege have the following additional rights (see section “Configuring openFT-AC” on page 30).

openFT V12 for BS2000 can be administered via the graphical user interface of openFT for Windows or openFT for Unix systems. It is possible to process the request queue, admission profiles, admission sets, logs, partner list and operating parameters.

As of openFT V12, it is also possible to set up a remote administration server via which you can administer other openFT instances from an openFT instance on a BS2000 system. See the chapter “Central administration” on page 99.

3.1 Optimizing the operating parameters

The proposals listed below suggest a number of ways in which the FT administrator can optimize FT operation by modifying the operating parameters. It is always advisable to alter only one operating parameter at a time, so that the precise effects of the change can be observed.

3.1.1 Interdependencies for optimized parameterization

The optimum settings for operating parameters depend on several different constraints:

- load levels of the local and remote systems,
- load level in the network,
- line transfer rates in the network,
- network structure (connection paths reserved for FT or shared paths for FT and dialog),
- incorporation of gateway computers (e.g. TRANSIT),
- type, performance or generation of the transport system used,
- average size of files to be transferred,
- number of files to be transferred (e.g. per day).

In some instances, these boundary conditions are themselves subject to dynamic change (load levels for example), so it is not possible to calculate in advance the optimized values for a particular installation.

3.1.2 Achieving optimized operation

Experience has shown that the most suitable parameter settings can only be achieved in stages.

Initially the openFT default values should be left unchanged. In most cases it will be possible to run file transfers satisfactorily using these parameter values.

If not, however, as a second step an improvement can be sought by changing **one** of the parameter values. It is normally not advisable to change more than one parameter at a time as otherwise there is no way of ascertaining the precise effect of each change.

If satisfactory operation of the FT system has still not been achieved, the FT administrator can repeat the second step, changing a different parameter.

The FT administrator can control the operation of the FT system using the parameters PROCESS-LIMIT, CONNECTION-LIMIT, TRANSPORT-UNIT-SIZE and MAX-REQUEST-LIFETIME, see the following table:

Problem	**Suggested solution**
Poor dialog response times	1. Reduce TRANSPORT-UNIT-SIZE 2. Reduce CONNECTION-LIMIT
Computer overloaded, network load not yet optimized	1. Set PROCESS-LIMIT to 2 2. Increase TRANSPORT-UNIT-SIZE 3. Reduce CONNECTION-LIMIT
Computer and network overloaded	1. Set PROCESS-LIMIT to 2 2. Reduce CONNECTION-LIMIT
Throughput inadequate	1. Increase TRANSPORT-UNIT-SIZE
Prolonged requests block other requests	1. Increase CONNECTION-LIMIT
Requests to a particular partner system use up all resources	1. Set the partner system to low priority with PRIORITY=*LOW 2. Increase CONNECTION-LIMIT 3. Set REQUEST-PROCESSING=*SERIAL for the corresponding partner system.
Requests from partner systems (inbound requests) use up all resources	1. Increase CONNECTION-LIMIT
Requests are present in the request file for a very long period without being processed.	1. Set MAX-REQUEST-LIFETIME

The command used for this purpose is MODIFY-FT-OPTIONS. These parameters are discussed in the sections below. In addition, the effect of changing the parameters is also described.

3.1.3 Changing the PROCESS-LIMIT operating parameter

The PROCESS-LIMIT parameter defines the maximum number of tasks that may be used for processing file transfer requests. The number of file transfer requests per task handled simultaneously can be expressed as follows:

$$\frac{\text{CONNECTION-LIMIT}}{\text{PROCESS-LIMIT}}$$

CONNECTION-LIMIT is the maximum number of parallel transport connections that can be used to execute requests.

If the PROCESS-LIMIT value remains fixed and the value of CONNECTION-LIMIT is increased, then proportionately more transport connections are available for each task and therefore more requests can be processed per task. The reduction of the PROCESS-LIMIT value where CONNECTION-LIMIT remains constant achieves the same effect. If the value of the quotient is reduced (by reducing CONNECTION-LIMIT or increasing PROCESS-LIMIT), a smaller proportion of transport links is available per task. Consequently, fewer requests can be processed per task.

If the number of requests awaiting processing exceeds the value of the quotient but the number of tasks assigned has not reached the PROCESS-LIMIT value, then another task is initiated.

The setting PROCESS-LIMIT=*NONE corresponds to the setting PROCESS-LIMIT= CONNECTION-LIMIT. A separate task is generated for each connection.

Higher PROCESS-LIMIT:

- fewer wait times for input/output
- better use of potentially underutilized computer resources

Lower PROCESS-LIMIT:

- reduced load on the local system

3.1.4 Changing the CONNECTION-LIMIT operating parameter

The CONNECTION-LIMIT parameter defines the maximum number of transport connections to be used in the execution of file transfer requests. Since the processing of a request always requires a new transport connection to be set up, CONNECTION-LIMIT also defines the maximum number of requests the system can process in parallel.

A third of the connections is reserved for outbound requests and a third for inbound requests. The remaining third can be used for inbound or outbound requests as required. You may therefore have to increase the value of CONNECTION-LIMIT to achieve the required throughput to your openFT partners.

Higher CONNECTION-LIMIT:

– increased data throughput

– better use of potentially underutilized processor capacity.

Lower CONNECTION-LIMIT:

– reduced load on the local system and network, and hence less or even no impact upon interactive operation.

3.1.5 Changing the TRANSPORT-UNIT-SIZE operating parameter

The TRANSPORT-UNIT-SIZE parameter defines the maximum length of the message transmitted to the transport system by openFT. TRANSPORT-UNIT-SIZE has no effect for links to FTAM partners. Message flow control ensures that only a specific number of messages are being transmitted across the network at any one time. The TRANSPORT-UNIT-SIZE parameter enables the administrator to control the amount of FT data per connection present in the network at a particular time. The value specified for TRANSPORT-UNIT-SIZE can be changed by the remote system or by the transport system (maximum message length).
A maximum value of 65535 is recommended for TRANSPORT-UNIT-SIZE. This value is the default value after installation.

Higher TRANSPORT-UNIT-SIZE:

- increased data throughput
- reduced load on the local system since fewer calls to the transport system are necessary.

Lower TRANSPORT-UNIT-SIZE:

- reduced load on the network
- the time required to transmit an FT message across a communication link is reduced, which in turn decreases the wait time for messages from other users. For slow communication links, response times can, for example, be improved in interactive mode.

3.1.6 Setting the MAX-REQUEST-LIFETIME operating parameter

The MAX-REQUEST-LIFETIME parameter is used to set a global limitation for the lifetime of openFT requests. The maximum lifetime applies to both inbound and outbound requests and is specified in days.

When this period expires, openFT deletes the request by executing the CANCEL-FILE-TRANSFER command internally (see page 147).

3.2 Administering code tables

The concept of so-called “Coded Character Sets” (CCS) is supported for openFT partners as of V10. A CCS defines a character set and the coding of these characters in the file. A CCS is assigned a name of up to 8 characters in length via which the CCS can be addressed.

When transferring text files, users can specify a separate CCS for file encoding in the local and remote systems (as of openFT V10).

Frequently used Coded Character Sets are:

ISO88591 Character set in accordance with the definition contained in ISO standard 8859-1, ASCII-oriented coding in accordance with ISO standard 8859-1.

EDF041 Character set in accordance with the definition contained in ISO standard 8859-1, EBCDIC-oriented coding in accordance with Fujitsu definition DF04-1.

UTF8 The character set is Unicode, the UTF-8 multi-byte coding defined in the Unicode standard is used.

UTF16 The character set is Unicode, the UTF16 16-bit coding defined in the Unicode standard is used.

CP1252 The character set is a superset, defined by Microsoft, of the character set defined in ISO standard 8859-1. The ASCII-oriented coding is identical to the ISO8859-1 for the characters which are shared with ISO8859-1.
The other characters defined by Microsoft (including the Euro symbol) are present in the code range 0x80-0x9F which is not used by ISO8859-1.

Making a CCS available

In BS2000/OSD, the CCSs are defined and made available via XHCS. The default CCS for the system (HOSTCODE) is defined by the BS2000 system administrator. The administrator can also assign a default user character set different to HOSTCODE to a user ID. As FT administrator, you must consult with the BS2000 system administrator to ensure that the required code tables are available on the system.

On the other openFT platforms as of V10, the commonly used CCSs are supplied with openFT. The FT administrator defines the default character set via the operating parameters.

3.3 Administering requests

You can use the SHOW-FILE-TRANSFER command (see page 284ff) to view information on selected FT requests. Possible selection criteria include

- the user ID,
- the system which initiated the request,
- certain statuses of FT requests, and
- names of file or job variables affected by an FT request in the local system.
- the pubset on which the transfer files are located.

The MODIFY-FILE-TRANSFER command permits both administrator and user to modify the order and priority of outbound requests within the request queue.

The CANCEL-FILE-TRANSFER command enables you to remote FT requests from the request queue or to abort file transfer while in progress. The selection criteria at your disposal are much the same as those for the SHOW-FILE-TRANSFER command. In particular, the FT administrator can purposely delete requests that lock files on a certain pubset (for example, if pubsets are to be reconfigured).

The FT administrator can use the CANCEL-FILE-TRANSFER ... FORCE-CANCELLATION command to force the full, unconditional cancellation of a request and its removal from the request file, if necessary without any negotiation with the partner system.

MODIFY-FT-PARTNER allows you to activate or deactivate locally submitted requests for a particular remote system (see STATE, page 251).

3.4 Administering partners

openFT offers the FT administrator four commands for the administration of partner systems:

ADD-FT-PARTNER	Add new partner system entries to the partner list
MODIFY-FT-PARTNER	Modify partner system entries in the partner list
REMOVE-FT-PARTNER	Remove partner systems from the partner list
SHOW-FT-PARTNERS	View information on partner systems in the partner list and back up the partner list (page 50)
START-OPENFTPART	Back up the partner list (page 50)
MODIFY-FT-OPTIONS	Enable/disable dynamic partners (page 43)

> For links with FTAM partners assumes that the transport system permits parallel connections. The remote systems are identified via their presentation addresses. Either BS2000 or the FTAM partner can initiate file transfer.

The partner list plays an important role during the administration of partners. A distinction is made between different types of partner system depending on whether and in what form partner systems are entered in the partner list.

3.4.1 Partner types

openFT recognizes three partner types:

- Named partners:
  All partners that are entered with their names in the partner list
- Registered dynamic partners:
  All partners that are entered without a name in the partner list
- Free dynamic partners:
  All partners that are not entered in the partner list

Registered dynamic partners and free dynamic partners are both simply referred to as dynamic partners.

Named partners

In FT requests, named partners are addressed using the names defined for them in the partner list.

You enter named partners in the partner list as follows:

```
ADD-FT-PARTNER PARTNER-NAME=name,PARTNER-ADDRESS=address...
```

These partners remain in the partner list until they are deleted from it using the REMOVE-FT-PARTNER command. If authentication is required for the connection to a partner then this partner should be entered in the partner list.

The use of named partners has the following advantages:

- Complex partner addresses do not have to be specified explicitly in openFT commands.
- Security is enhanced because only partners that are genuinely recognized can be permitted.
- Partner authentication is possible

i Although a named partner can also be connected to via its address, in all openFT tasks such as logging or request queue activities, the partner name is displayed.

Registered dynamic partners

All partners that are entered only with their addresses but without names in the partner list are registered dynamic partners. They can only be accessed via the address and possess at least one attribute that differs from the default value for a free dynamic partner (see section “Free dynamic partners” on page 43).

You enter partners of this type in the partner list as follows:

```
ADD-FT-PARTNER PARTNER-NAME=*NONE
                   ,PARTNER-ADDRESS=address,<other attributes>.
```

I.e., you assign one or more attributes with a value other than the default, e.g. TRACE=*ON.

Please note:

- Security level based on the partner setting (SECURITY-LEVEL=*BY-PARTNER-ATTRIBUTES) is the default setting for free dynamic partners and therefore does not count as a differently set attribute.
- In contrast, security level based on the operating parameter setting (SECURITY-LEVEL=*STD; default setting for the ADD-FT-PARTNER command) is a differently set attribute.

If you reset all the attributes for a partner of this type to the default values with MODIFY-FT-PARTNER then this partner is removed from the partner list and becomes a free dynamic partner.

Free dynamic partners

Free dynamic partners are all the partners that are not entered in the partner list. They are therefore not displayed when you enter SHOW-FT-PARTNERS without specifying a partner name or partner address.

Partners of this type can only be connected to via their address and, with the exception of SECURITY-LEVEL, possess the default attributes as described in the command ADD-FT-PARTNER. The SECURITY-LEVEL for a free dynamic partner is *BY-PARTNER-ATTRIBUTES (and not *STD).

For the meaning of these attributes, see the ADD-FT-PARTNER or MODIFY-FT-PARTNER commands.

You can use the MODIFY-FT-PARTNER command to transform a free dynamic partner into a registered dynamic partner:

```
/MODIFY-FT-PARTNER address,<other attributes>
```

Enter a partner address that does not refer to any existing partner list entry and define one or more attributes with values other than the default (see above). You do not specify the PARTNER-ADDRESS operand.

The advantage of the free dynamic partner concept is that users can address any required partners that are not entered in the partner list. This reduces the administrator's workload in terms of administration requirements. The disadvantage lies in the increased security risk and is the reason why you are also able to prohibit the use of dynamic partners, see below.

i If the status of a free dynamic partner changes (for example, in NOCON= partner not available) and is therefore different from the default value then it is displayed in the partner list. However, it becomes a free dynamic partner again as soon as it once more becomes accessible (ACTIVE status).

Activating/deactivating dynamic partners

As system administrator, you may also prohibit the use of dynamic partners for security reasons. To do this, enter the following command:

```
/MODIFY-FT-OPTIONS ... DYNAMIC-PARTNERS=*OFF
```

In this case, it is necessary to address partners via their names in the partner list. They cannot be addressed directly via their address. Inbound access is then also only permitted to partners that are entered with a partner name in the partner list.

You can use MODIFY-FT-OPTIONS ... DYNAMIC-PARTNERS=*ON to permit dynamic partners again.

3.4.2 Defining partner properties

You use the ADD-FT-PARTNER command to define the properties of partners:

- Partner address, see page 44
- FTAC security levels, see page 48
- Automatic deactivation and Inbound deactivation, see page 49
- Serialization of asynchronous outbound requests, see page 49
- Partner-specific trace settings, see page 91
- Authentication setting and instance identification for the partner, see page 53
- Sender verification, see page 60
- Priority, see page 141.

You can modify these settings whenever you want with MODIFY-FT-PARTNER.

3.4.2.1 Specifying partner addresses

The following applies to the addressing of partner systems:

- the partner address complies with internet address conventions, see “Structure of the partner address”. You specify the partner address as in the past in the ADD-FT-PARTNER or MODIFY-FT-PARTNER command.
- a partner can be accessed directly via its address in FT requests even if it is not entered in the partner list. This is only possible if the “dynamic partner” function is enabled, see page 43.
- It is also possible to address ftp partners.

Structure of the partner address

A partner address has the following structure:

[protocol://]host[:[port].[tsel].[ssel].[psel]]

host (= computer name or processor name, see page 45) is mandatory; all other specifications are optional. In many cases, the other specifications are covered by the default values, so that the host name suffices as the partner address, see “Examples” on page 47. Final ’.’ or ’:’ can be omitted.

The individual components of the address have the following meanings:

protocol://

Protocol stack via which the partner is addressed. Possible values for *protocol* (uppercase and lowercase are not distinguished):

openft openFT partner, i.e. communication takes place over the openFT protocol.

ftam FTAM partner, i.e. communication takes place over the FTAM protocol.

ftp FTP partner, i.e. communication takes place over the FTP protocol.

ftadm ADM partner, i.e. communication takes place over the FTADM protocol for remote administration and ADM traps.

Default value: **openft**

host

Computer name via which the partner is addressed. Possible entries:

- BCAM processor name, length 1 to 8 characters
- only with FTP partners:
  - internet host name (e.g. DNS name), length 1 to 80 characters
  - IPv4 address with the prefix %ip, i.e. for example %ip139.22.33.44

    The IP address must always be specified as a sequence of decimal numbers separated by dots and without leading zeros.
  - IPv6 address with the prefix %ip6, i.e. for example `%ip6[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]` (ipv6) or `%ip6[FE80::20C:29ff:fe22:b670%5]` (ipv6 with scope ID)

    The square brackets [..] must be specified.

    The scope ID designates the local network card via which the remote partner can be accessed in the same LAN-Agment. It must be appended to the address with a % character. In Windows systems, this is a numerical value (e.g. 5). On other systems, it may also be a symbolic name (e.g. *eth0*). The scope ID can be identified using the *ipconfig* command.

    i When the SHOW-FT-PARTNERS command is issued, openFT attempts to determine the DNS name and displays this instead of the IPv4-/IPv6 address.

port

When a connection is established over TCP/IP, you can specify the port name under which the file transfer application can be accessed in the partner system.
Permitted values: 1 to 65535;

Default value: **1100** for openFT partners
A different default value can also be set in the operating parameters using MODIFY-FT-OPTIONS.

4800 for FTAM partners

21 for FTP partners

11000 for ADM partners

tsel

Transport selector under which the file transfer application is available in the partner system. The transport selector is only relevant for openFT and FTAM partners.
You can specify the selector in printable or hexadecimal format (0xnnnn...). The specification will depend on the type of partner:

– openFT partner:
Length 1 to 8 characters, alphanumeric characters and the special characters # @ $ are permitted. A printable selector will be coded in EBCDIC in the protocol and may be padded with spaces internally to the length of eight characters.

Default value: **$FJAM**

– FTAM partner:
Length 1 to 16 characters; a printable selector will be coded as variable length ASCII in the protocol. Exception: T selectors that start with $FTAM (default value) are coded in EBCDIC and padded with spaces to the length of 8 characters.

All alphanumeric characters and the special characters @ $ # _ - + = and * can be used with ASCII selectors.

Default value: **$FTAM**

Note
As a rule, **SNI-FTAM** must be specified for Windows partners with openFT-FTAM up to V10. As of openFT-FTAM V11 for Windows, the default value has been changed to **$FTAM** and can therefore be omitted.
Printable transport selectors are always used in uppercase in openFT even if they are specified or output in lowercase.

ssel

Session selector under which the file transfer application is accessible in the partner system. You can specify the selector in printable or hexadecimal format (0xnnnn...).

Length 1 to 16 characters, alphanumeric characters and the special characters @ $ # _ - + = * are permitted. A printable selector will be coded as variable length ASCII in the protocol.

Default value: empty

Note:
Printable session selectors are always used in uppercase in openFT even if they are specified or output in lowercase.

psel
Only relevant for FTAM partners.
Presentation selector under which the file transfer application is accessible in the partner system. You can specify the selector in printable or hexadecimal format (0xnnnn...).

Length 1 to 16 characters, alphanumeric characters and the special characters @ $ # _ - + = * are permitted. A printable selector will be interpreted as variable length ASCII in the protocol.

Default value: empty

Note:
Printable presentation selectors are always used in uppercase in openFT even if they are specified or output in lowercase.

Examples

The partner computer with the host name FILESERV is to be addressed over different protocols/connection types:

Connection type/protocol	**Address specification**
openFT partner	FILESERV
FTAM partner (BS2000, Windows or Unix system with default setting as of V11.0)	ftam://FILESERV
FTAM partner (Windows system with default setting up to V10.0)	ftam://FILESERV:.SNI-FTAM
Third-party FTAM partner	ftam : / /FILESERV:102.TS0001.SES1.PSFTAM
FTP partner	ftp://FILESERV

You find more examples in the sections “Sample openFT partner entries” on page 143, “Sample FTAM partner entries” on page 144, and “Examples for entering FTP partners” on page 146.

3.4.2.2 FTAC security levels for partners in the partner list

If the FTAC functionality is to be used, the FT administrator should - in cooperation with the FTAC administrator - additionally define the appropriate FTAC security level for each partner entry using the command ADD-FT-PARTNER or MODIFY-FT-PARTNER (operand SECURITY-LEVEL).

The security levels regulate the degree of protection with respect to the partner system. A high security level is used when a high degree of security is required, and a low level for a low degree of security. When FTAC is first used, the security levels should be assigned in multiples of ten. This leaves the option open to incorporate new partner systems flexibly into the existing hierarchy.

If the degree of required security changes with respect to a partner system, the security level of the partner system can be modified with the command MODIFY-FT-PARTNER to meet the new requirements.

You can also use the operand SECURITY-LEVEL=*BY-PARTNER-ATTRIBUTES to activate the following automatic mechanisms for the security levels:

- Partners that are authenticated by openFT are assigned security level 10.
- Partners that are known in BCAM (i.e. they are addressed via their BCAM name) are assigned security level 90.
- Partners which are accessed via their IP address (only possible in the case of FTP) are assigned security level 100.

This automatic mechanism can be activated on a partner-specific basis (ADD-FT-PARTNER and MODIFY-FT-PARTNER) or globally by means of MODIFY-FT-OPTIONS.

If you have specified SECURITY-LEVEL=*STD for the partner then openFT uses the global settings in the operating parameters. Here, it is also possible to specify a fixed security level as the default.

For information on when the security level of a partner entry is of importance, see section “Administrating and controlling FTAC functions” on page 80.

3.4.2.3 Outbound and inbound deactivation

You can deactivate named partners specifically for asynchronous outbound requests or for inbound requests.

In addition, you can enable the automatic deactivation for outbound requests so that the partner is disconnected for outbound requests after five failed attempts to establish a link. This prevents unnecessary costs from arising in the case of certain link types, such as DATEX-P, which also charge for unsuccessful link establishment attempts. Automatic deactivation does not work when the attempt fails due to an error in the BCIN commands in the local system, but neither are any costs incurred in such a case. Before any new attempts are made, the system must be manually reactivated.

You can assign these settings either with the ADD-FT-PARTNER command when setting up the partner system or subsequently by means of the MODIFY-FT-PARTNER command.

3.4.2.4 Serialization of asynchronous outbound requests

You can force the serialization of asynchronous outbound requests for a partner system (REQUEST-PROCESSING=*SERIAL in ADD-FT-PARTNER and MODIFY-FT-PARTNER).

This prevents the "overtaking" effects that can arise when requests are processed in parallel. The following points apply to serial processing:

- A follow-up request is not started until the preceding request has terminated.
- Serialization includes preprocessing and postprocessing operations but not follow-up processing operations because these are independent of the request.

This function can be used, for example, in a branch-head office configuration in which the branches send multiple files to the head office at the same time (daily, weekly or monthly figures). If serialization is enabled for the partner "head office" in the branch computers then each branch computer can only have only one active connection to the head office computer at any one time. This prevents bottlenecks at the head office computer of the sort that occur, for example, if the CONNECTION-LIMIT is regularly exceeded.

3.4.3 Backing up the partner list

You can back up the entries in the partner list by means of the SHOW-FT-PARTNERS command or the START-OPENFTPART command:

- SHOW-FT-PARTNERS outputs the partner entries in the form of MODIFY-FT-PARTNER commands. To do this, specify the
  OUTPUT=*SYSLST(LAYOUT=*BS2-PROC) operand.

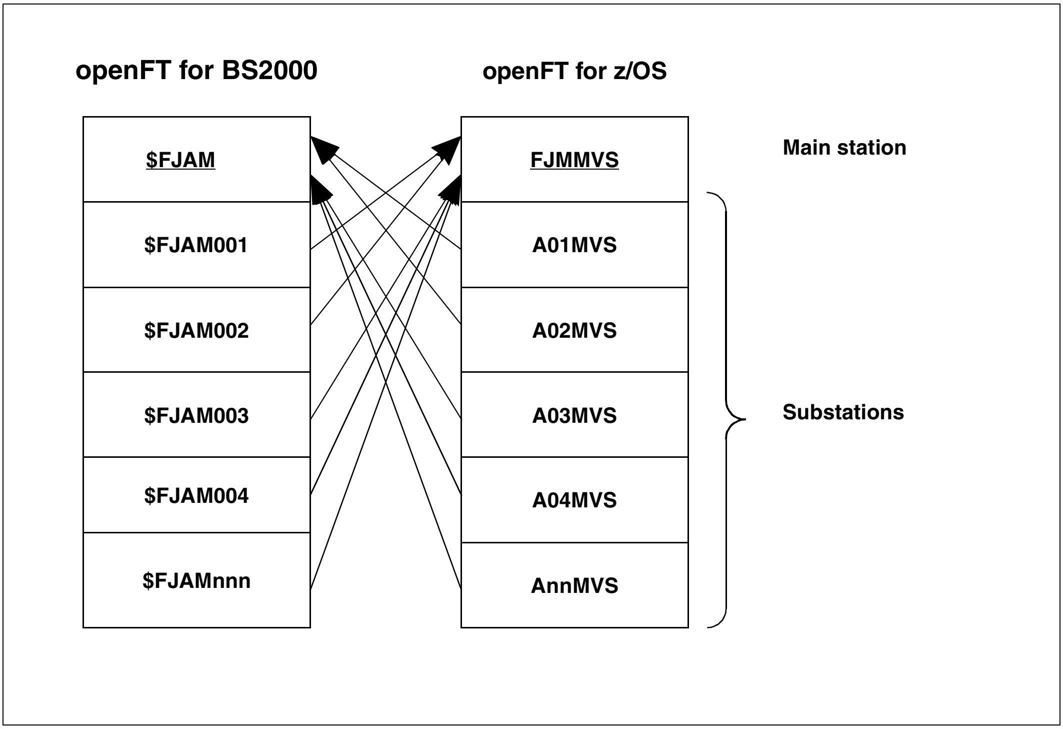
  The output can be redirected to a file by means of the ASSIGN-SYSLST command. To make the procedure executable, the first column of the output file must then be removed in an editor.

- START-OPENFTPART also outputs the partner entries to a file in the form of MODIFY-FT-PARTNER commands with the difference that the first column is already removed.

3.4.4 Addressing concept for partners up to openFT V8.0

In some transport systems, it is not possible to have multiple and concurrent transport connections between the same end points. In order to handle multiple FT requests simultaneously between two FT systems, all FT products up to V8.0 have a standardized addressing concept which is described below. As of openFT V9.0 for BS2000 or z/OS and openFT V8.1 for Unix systems or Windows systems, this addressing concept is superseded by network-wide, unique instance IDs for the openFT instances (see section "Using openFT in a HIPLEX cluster" on page 88). Compatibility is also provided for, so that you can link new and old versions together based on the previous addressing concept, without any problems.

In the traditional addressing concept, there is a so-called main station (main application) in each openFT system which serves as the end point for all links that are initiated in partner systems. The starting points for links to partner systems are the so-called substations (subapplications) in the local system.
The following diagram illustrates this principle, using the coupling of openFT for BS2000 and openFT for z/OS and OS/390 as an example:



Main station and substations

The main station of the partner system is entered in the partner list with the aid of the ADD-FT-PARTNER command (default value: $FJAM).

If openFT is used with the extended authentication check facility for openFT partners (PARTNER-CHECK=*TRANSPORT in the MODIFY-FT-OPTIONS and ADD-FT-PARTNER commands), the transport address of the partner is also checked against the entry in the partner list. The originator, however, is always one of the substations of an FT system, although it is the main station of the partner system that is entered in the partner list. This is the reason why naming conventions must be applied to ensure correct assignment. openFT partners that do not adhere to these naming conventions are rejected when extended authentication checking is in operation.

openFT recognizes two naming conventions:

1. If “$FJAM” was entered for the main station of the remote system (default value for BS2000 partners and computer interconnection with Unix partners), any substation specification in the form “$FJAM*nnn*” is accepted, where *nnn* may be any three-digit number. The main station of openFT for BS2000 is always “$FJAM” and the associated substations are designated as described above without additional work being required at generation.
2. FJM*ftid* is entered as the main station of the partner system. *ftid* is a five-character alphanumeric string and must be unambiguous throughout the network.
   The substations are designated A*nnftid*, *nn* being two-digit numbers. *ftid* has the same meaning as for the main station. *ftid* must be the same for the main station and all its associated substations.

3.5 Security in FT operation

A user wanting to access resources of a system must always provide the system with proof of his or her authorization for the access. In the case of file transfer activities, access authorization must be verified in both the local and the remote system. Verification usually entails specifying a user ID and a corresponding password.

The following functions offer an even higher level of security in file transfer:

- Authentication
- Encryption during data transfer, see page 61
- Use of FTAC functions by means of openFT-AC, see page 80

In addition, openFT provides an extended sender verification function (see page 60) that can be used, for example, if it is not possible to work with authentication, as well as mechanisms that protect against file inconsistencies (see page 62).

3.5.1 Authentication

If data requiring a high degree of security is to be transferred, it is important to subject the respective partner system to a reliable identity check ("authentication"). The two openFT instances taking part in a transfer must be able to cryptographically check one another to determine whether they are connected to the "correct" partner instance.

Therefore, as of versions openFT V8.1 for Unix systems and Windows systems, and V9.0 for BS2000 and z/OS, an expanded addressing and authentication concept is supported for openFT partners. It is based on the addressing of openFT instances using a network-wide, unique ID and exchanging partner-specific key information.

You should note that authentication in openFT for BS2000 is only possible for named partners!

When communicating with partners that are still using openFT version 8.0 (or earlier), the functions described in the following are not usable. For the sake of compatibility, the previous addressing concept is still supported for these partners. For FTAM partners and FTP partners, authentication is not available in this form, since the neither the FTP protocol nor the FTAM protocol standardized by the ISO provide a comparable functionality.

3.5.1.1 Usages of the authentication

There are three distinct usages of the authentication:

- Case 1:
  The local openFT instance checks the identity of the partner instance. This assumes that a current, public key of the partner instance was stored locally, see section "Managing the keys of partner systems" on page 58.
  This sort of configuration makes sense, for example, if files on a file server are to be accessed using openFT. It is important for the local openFT instance, that the retrieved data should come from a reliable source (from the authenticated partner). In contrast, the file server is not concerned with who is accessing it.
- Case 2:
  The partner instance checks the identity of the local openFT instance. This assumes that a current, public key of the local openFT instance is stored in the partner instance (re-coded - for Unix and Windows partners), see sections "Creating and managing local RSA key pairs" on page 56 and "Distributing the keys to partner systems" on page 59.
  This sort of configuration would be considered, for example, if partner systems in several branch systems are to be accessed using openFT from a central computer, and where the branch system computers only allow the central computer access (and, in practice, only the central computer).
- Case 3:
  Both of the openFT instances engaged in a transfer authenticate each other (combination of case 1 und case 2). This assumes that current, public keys were mutually exchanged and the partners are addressing each other using their instance IDs. In this way, it can be ensured that the data not only comes from a reliable source, but that it will also end up in reliable hands

In the case of configuration errors that inhibit the authentication of one of the partners participated in the request no session is created which can execute the request. The request is not started. Hence, the problem cannot be found out by means of the request state. The partner state (RAUTH or LAUTH) shows on which side the problem was recognized.

3.5.1.2 Instance identifications

The instance ID is a unique name, up to 64 characters long. Its uniqueness **within the network** must be based on something other than case-sensitivity. It is particularly important if you are working with authentication.

During installation, the name of the real BCAM host is defined by default as the instance ID. If it cannot be guaranteed that this name is unique in the network then you must change the instance ID. To do this, enter the command: MODIFY-FT-OPTIONS with the IDENTIFICATION operand.

Modifying local instance identification

An instance ID may be comprised of alphanumeric characters and the special characters. You are advised only to use the special characters “.”, “-”, “:” or “%”. The first character must be alphanumeric or the special character “%”. The “%” character may only be used as a first character. An alphanumeric character must follow a “.” character.

In order to ensure the network-wide uniqueness of instance IDs, you should proceed as follows when assigning them:

- If the openFT instance has a network address with a **DNS name**, you should use this as the ID. You can create an “artificial” DNS name for an openFT instance, by placing part of a name, separated by a period, in front of an existing “neighboring” DNS name.
- If the openFT instance does not have a DNS name, but is connected to a TCP/IP network, you should use the ID **%ipn.n.n.n** (n.n.n.n is the IP address of the local openFT instance, minus the leading zeros in the address components).
- If the openFT instance is connected to an ISDN network rather than a TCP/IP network, you should use the ID **%isdnmmmmmmmm** (mmmmmmmm is the ISDN call number, including country and local prefixes).
- If the openFT instance is connected to an X.25 network (but not to TCP/IP or ISDN), the ID should begin with **%x25** and the X.25 number should contain the NSAP, where necessary (e.g. **%x25mmmmmmmmmmNSAP)**.

The form of instance ID used internally by openFT for partners using a version earlier than V8.1, (i.e. **%.<prozessor>.<entity>)**, should not be used for your own openFT instance.

Instance identification of partners

Store instance IDs of partner systems in the partner list using the IDENTIFICATION parameter of the ADD-FT-PARTNER command, or MODIFY-FT-PARTNER. With the aid of the partner systems’ instance IDs, openFT manages the resources assigned to those partners, such as request hold queues and cryptographic keys.

3.5.1.3 Creating and managing local RSA key pairs

RSA keys are used for authentication as well as for the negotiation of the AES key with which the request description data and file contents are encrypted.

You can use the following commands to generate and manage local RSA key.

CREATE-FT-KEY-SET	creates an RSA key pair set for the local openFT instance
SHOW-FT-KEY	shows the attributes of all keys in the local system
UPDATE-FT-PUBLIC-KEYS	updates the public keys
DELETE-FT-KEY-SET	deletes local RSA key pair sets
MODIFY-FT-KEY	modifies RSA key attributes
IMPORT-FT-KEY	imports RSA keys

Key pair attributes

Each RSA key pair consists of a private and a public key. There can be up to three key pair sets each consisting of three key pairs with lengths of 768, 1024, 2048. The CREATE-FT-KEY-SET command generates new key pairs for each of these lengths.

Private keys are internally administered by openFT. Public keys are stored on the configuration user ID of the openFT instance (standard: $SYSFJAM), under the following name:

```
SYSPKF.R<key reference>.L<key length>
```

The key reference is a numeric designator for the version of the key pair.

The public key files are text files, which are created in the character code of the respective operating system, i.e. EBCDIC.DF04-1 for BS2000 and z/OS, ISO8859-1 for Unix systems and CP1252 for Windows systems.

i A key of length 2048 is used by default for encryption. You can modify this setting using the MODIFY-FT-OPTIONS command.

Storing comments

In a SYSPKF.COMMENT file on the configuration user ID of the openFT instance, you can store comments, which are written in the first lines of the public key files when a key pair set is created. Comments could, for example, contain the contact data for the FT administrator on duty, the computer name, or similar information that is important for partners. The lines in the SYSPKF.COMMENT file may be a maximum of 78 characters in length. Using the UPDATE-FT-PUBLIC-KEYS command, you can import updated comments from this file into existing public key files at a later time.

Updating and replacing keys

If a public key file has been unintentionally deleted or otherwise manipulated, you can recreate the public key files of the existing key pair sets using UPDATE-FT-PUBLIC-KEYS.

If you want to replace a key pair set with a completely new one, you can create a new key pair set using CREATE-FT-KEY-SET. You can identify the most current public keys by the highest value key reference in the file name. *Open*FT supports a maximum of three key pair sets at a time. The existence of several keys should only be temporary, until you have made the most current public keys available to all the partner systems. Afterwards, you can delete the key pair sets no longer needed using DELETE-FT-KEY-SET.

If the openFT administrator is not the same as the system administrator, it must be ensured that this administrator has access to the SYSPKF files and the SYSKEY library on the configuration user ID of the openFT instance. This can be done, either by assigning operating system-specific access rights or by setting up corresponding FTAC admissions profiles.

3.5.1.4 Importing keys

You can use the IMPORT-FT-KEY command to import the following keys:

- Private keys that were generated with an external tool (i.e. not via openFT). When importing a private key, openFT generates the associated public key and stores it under the configuration user ID of the openFT instance, see “Key pair attributes” on page 56. This key can be used in the same way as a key generated with CREATE-FT-KEY-SET and distributed to partner systems.
- Public keys of partner instances. These keys must have the openFT key format (syspkf), i.e.. they must have been generated by the partner's openFT instance. openFT stores the key in the SYSKEY library, see “Managing the keys of partner systems” on page 58.

Every imported key pair contains a unique reference number. RSA keys with the supported key lengths are imported (768, 1024 and 2048 bits).

openFT supports key files in the following formats:

- PEM format (native PEM)

  The PEM-coded files must be present in EBCDIC format.
- PKCS#8 format encrypted without password phrase or after v1/v2 with password phrase (PEM-coded).

  You must specify the password phrase used for encryption in the password parameter when you perform the import.

- PKCS#12 v1 format in the form of a binary file. The file is searched for a private key and any non-supported elements (e.g. certificates, CRLs) are ignored during the import. If the certificate is protected by a signature or hash then openFT does not perform a validity check. The validity of the file must be verified using other means. The first private key that is found in the file is imported. Any others are ignored.

  You must specify the password phrase used for encryption in the password parameter when you perform the import.

3.5.1.5 Managing the keys of partner systems

The public keys of the partner systems are to be stored in BS2000 as type D PLAM elements in the **SYSKEY** library on the configuration user ID of the local openFT instance. The partner name of the partner system as defined in the partner list must be selected as the element name. If an updated public key is made available by the partner instance, the old key must be overwritten by it.

You can import the public key of a partner system in the following ways:

- You can specify the name of the key file in the IMPORT-FT-KEY command. When you perform the import, openFT checks whether there is a partner list entry with the instance ID that is stored in the key file. If there is then openFT stores the key under the partner's name in the SYSKEY library.
- You can use the tools available in the operating system to copy the key file in the correct format to the SYSKEY library and save it there under the partner's name.

If an updated public key is made available by the partner instance, the old key must be overwritten by it.

overwritten by this

You can use the command SHOW-FT-KEY ...SELECT=*PAR(PARTNER-NAME=...) to display the keys of partner systems and filter on expiration date.

Modifying the keys of partner systems

You can use the MODIFY-FT-KEY command to modify the keys of partner systems by specifying an expiration date or modifying the authentication level (1 or 2):

- If you specify an expiration date then it is no longer possible to use the key once this date has expired.
- If you set authentication level 2 then openFT also performs internal checks. Level 2 is supported for all openFT partners as of Version 11.0B. Level 1 authentication attempts to this partner are rejected.

You can make these settings for a specific partner or for all partners, as you require, and modify them subsequently if necessary.

3.5.1.6 Distributing the keys to partner systems

Distributing the public key files to your partner systems should take place by secure means, for example by

– distribution by cryptographically secure e-mail
– distribution on a CD (by courier or by registered mail)
– distribution via a central openFT file server, the public keys of which are in the partners' possession

If you transmit your public key files to partner systems using Unix or Windows operating system, you must ensure that these files are re-coded from EBCDIC.DF04-1 to ISO 8859-1 or CP1252 (e.g. by transferring them as a text file via openFT).

The public key file of your local openFT instance is stored in the partner system in the following location:

– For partners with openFT for BS2000, as a type D PLAM element in the **SYSKEY** library, the configuration user ID of the partner instance. The partner name allocated for your openFT instance in the remote network description file or in the remote partner list must be selected as the element name.

– For partners with openFT for Unix systems, in the **/var/openFT/<instance>/syskey** directory. The instance ID of your local openFT instance must be selected as the file name. The file name must not contain any uppercase letters. If the instance ID contains uppercase letters, these must be converted to lowercase in the file name.

– For partners with openFT for Windows, in the directory <**openFT installation directoy>\var\<Instance>\syskey**, as of Windows Vista in **%ProgramData%\Fujitsu Technology Solutions\openFT\var\std\syskey**.
The instance ID of your local openFT instance must be selected as the file name.

– For partners with openFT for z/OS or OS/390, as a PO element in the **<admuser>.SYSKEY** library. The partner name allocated for your openFT instance in the remote network description file or partner list must be selected as the element name.

3.5.2 Extended authentication check

openFT partners using openFT from version 8.1 onwards, support the authentication mechanism (see page 53). If the local system has a public key of the partner at its disposal, the partner's identity is checked by cryptographic means.

For partner systems that do not work with authentication, inbound requests are checked with the aid of the instance identification, in order to ascertain whether the calling system has a valid entry in the partner list. openFT offers via extended sender checking the possibility of checking not only the instance identification, but also the transport address.

The extended sender checking can be globally enabled for openFT partners or just for specific partners:

- globally, using
  MODIFY-FT-OPTIONS... PARTNER-CHECK=*TRANSPORT-ADDRESS
- only for specific partners, using
  ADD-FT-PARTNER ... PARTNER-CHECK=*TRANSPORT-ADDRESS or
  MODIFY-FT-PARTNER ... PARTNER-CHECK=*TRANSPORT-ADDRESS

The global setting is valid for all partners with the value PARTNER-CHECK=*BY-FT-OPTIONS (default in the ADD-FT-PARTNER).

In the case of FTAM and FTP partners, the sender check operates exclusively via the transport address. Consequently the "extended sender verification" attribute is ineffective for FTAM and FTP partners and is also not displayed.

Extended sender verification is of no relevance for dynamic partners because these are always identified via the transport address.

If the authentication check returns a negative result, the request is rejected.

3.5.3 Encryption for file transfer

openFT supports for openFT partners the encryption of the data sent and received in the process of setting up the connection and processing a file transfer request. The partners involved in file transfer automatically negotiate encryption and use of the appropriate public key in the process of connection set-up.

If possible, openFT uses the RSA/AES procedure with a key length of 256 bits for encryption. In the case of connections with older partners, 128-bit RSA/AES or RSA/DES may also be used. In all cases, the most secure of the procedures that are supported by both partners is used.

openFT automatically encrypts the request description data if both partners support this functionality, there is an RSA key pair set in the local system and encryption has not been explicitly disabled (command MODIFY-FT-OPTIONS ...KEY-LENGTH=0). You can use the SHOW-FT-OPTIONS command to check the key length that is currently being used (output parameter KEY-LEN). You can set the key length required for the RSA key via the operating parameters (MODIFY-FT-OPTIONS command KEY-LENGTH parameter).

Using the CREATE-FT-KEY-SET command, the FT administrator must create at least one key pair set, upon which the encryption will be based and carried out. Alternatively, the administrator can also import a key pair of the configured key length using IMPORT-FT-KEY.

If, in addition to the request description data, the file content is to be encrypted for transfer by openFT, then the optional openFT-CR component must be installed on both FT systems involved.

If one of the two systems is not capable of handling encrypted file transfers, the request is rejected with the message FTR2051 (no openFT-CR in local system) or with FTR2113 (encryption is not possible in remote system).

For legal reasons, openFT-CR is not available in all countries.

In BS2000, if the openCRYPT subsystem is installed and started in addition to openFT-CR, then openFT itself does not encrypt the file content, but allows openCRYPT to handle the encryption. This considerably enhances performance.

Forcing encryption

Encryption of the file contents is optional and is usually requested during the transfer request. However, you can also use the operating system parameters to force encryption (mandatory encryption). To do this, use the ENCRYPTION-MANDATORY operand in the MODIFY-FT-OPTIONS command.

Mandatory encryption can be set differently for different operations (only inbound, only outbound or all requests). The settings apply to file transfer requests via the openFT protocol as well as for administration requests. FTAM requests and inbound FTP requests are rejected because no encryption is permitted. File management continues to be performed irrespective of the settings. In addition, the following applies:

- If outbound encryption is activated then the file content is encrypted on outbound requests even if no encryption is demanded in the request itself. If the partner does not support encryption (e.g. because it is deactivated or because openFT-CR is not installed) then the request is rejected.
- If an unencrypted inbound request is to be processed while inbound encryption is activated, then this request is rejected.

3.5.4 Protection mechanisms against data manipulation

Prior to version V8.0, FT products in BS2000 protected a file to be transferred only during the active transmission, i.e., when the file was opened by openFT using DVS. Consequently, if the transmission was interrupted or even if the transmission had not yet begun, both files involved could be potentially accessed and modified. Such changes could not always be detected on restarting openFT, thus resulting in the creation of inconsistent receive files.

As of V8.0, openFT uses an operating system mechanism to protect transfer files (however, this protection is not possible for library elements and Posix files):

- When a file transfer request is accepted, a lock is set on each file to be transferred as early as possible. Only read access is granted to other users for the send files; no access is permitted for the receive files.
- This lock remains set - so long as the FT subsystem is loaded - until the request has completed.
- The BS2000 command SHOW-FILE-LOCK indicates whether a file has been locked by openFT and, if it is, shows the transfer ID (or, when sending, possibly a list of transfer IDs) of the request involved. Such locks, and other file locks as well, can be reset by the system administrator at his/her own discretion in emergency situations by using the command REMOVE-FILE-ALLOCATION.
- Using SHOW-FILE-TRANSFER ... PUBSET=, the FT administrator can have all the requests displayed that have locked files on a defined pubset. The administrator can selectively delete these requests using CANCEL-FILE-TRANSFER ... PUBSET=.

On unloading an FT instance (STOP-SUBSYSTEM FT or DELETE-FT-INSTANCE), all the locks held by openFT are cleared and reset upon reload (START-SUBSYSTEM FT or CREATE-FT-INSTANCE) for all files affected by existing requests. For information on what the FT or system administrator must therefore take into consideration, see section “Starting and stopping openFT” on page 28.

In addition to this mechanism, openFT also implicitly checks the integrity of the transferred data by communicating with openFT partners version V8.1 and later. The scope is defined in the transfer request:

– In the case of requests with encryption, the transferred file content is also checked (TRANSFER-FILE ... DATA-ENCRYPTION = *YES).

– In the case of requests without encryption, an integrity check of the file content can be activated explicitly
(TRANSFER-FILE ... DATA-ENCRYPTION = *ONLY-DATA-INTEGRITY.

– If neither encryption nor the integrity check are activated then only the integrity of the request description data is checked
(TRANSFER-FILE ... DATA-ENCRYPTION = *NO).

If an error is detected then restartable requests attempt the transfer again. Requests that cannot restart are aborted.

3.6 Monitoring and controlling FT operation

Fetch information on the FT system

The FT administrator uses the following commands to obtain information on the system:

SHOW-FT-OPTIONS	Information on operating parameters
SHOW-FT-PARTNERS	Information on partner systems
SHOW-FT-LOGGING-RECORDS	Information on log entries
SHOW-FILE-TRANSFER	Information on file transfer status
SHOW-FT-INSTANCE	Information on openFT instances
SHOW-FT-MONITOR-VALUES	Show monitoring data from openFT operation

The SHOW-FT-OPTIONS command furnishes information on the current settings of the operating parameters.

SHOW-FT-PARTNERS yields information on the partner systems and their associated properties, e.g., names, addresses, security levels for FTAC, and so on. The command and the possible outputs are described in detail starting on page 363.

To support automatic monitoring, some events which are not direct responses to user input are reported by openFT via console messages. More detailed information on this topic can be found in the section “Console messages for automatic monitoring” on page 68.

The command SHOW-FT-LOGGING-RECORDS can be used to display the logs of file transfer requests. You will find more information on this subject in the section below and in the description of the SHOW-FT-LOGGING-RECORDS command on page 315ff.

SHOW-FILE-TRANSFER enables the FT administrator to retrieve information on all file transfer requests in his or her system, even when the FT system is stopped.

Using SHOW-FT-INSTANCE, the FT administrator can find out which openFT instances exist in the system and have their characteristics and status displayed.

SHOW-FT-MONITOR-VALUES outputs the monitoring values from openFT operation. To do this, monitoring must be activated by means of MODIFY-FT-OPTIONS.

3.6.1 FT logging

The following 3 commands are available for the FT logging function:

DELETE-FT-LOGGING-RECORDS	– Deleting log records
	– Deleting offline log files
MODIFY-FT-OPTIONS	– Switching on/off the logging function and define the scop of logging
	– Changing the log file
	– Define whether log entries are to be regularly deleted and, if necessary, specify the deletion interval.
SHOW-FT-LOGGING-RECORDS	– View information on log entries
	– Listing log file names

openFT can record the results of all file transfer requests, irrespective of whether the initiative is in the local or the remote system (outbound and inbound requests, respectively). The information on each successfully completed or aborted request is recorded in an FT logging record. The file consisting of these logging records thus represents a complete, uninterrupted documentary record of FT operation over a prolonged period of time.

openFT writes the logging records into the log file SYSLOG.Lyymmdd.Lhhmmss on the configuration user ID of the openFT instance (default: $SYSFJAM).

yy = year, 2-digit.
mm = month, 2-digit.
dd = day, 2-digit.
hh = hour, 2-digit.
mm = minute, 2-digit.
ss = second, 2-digit.

The date and time designate the time (GMT) at which the log file was created. This suffix makes it possible to distinguish between the current and offline log files.

The SYSLOG files are created by the FT system with second allocation 500, its net size depends on the number of logging records it contains.

Changing the log file and administering offline log files

You can change the log file using the MODIFY-FT-OPTIONS LOGGING=*CHANGE-FILES command. This closes the current log file which is nevertheless retained as an offline log file. For the following log records, a new log file is created with the current date in the suffix. You can change the log file several times and therefore manage multiple offline log files.

This change-over has the following benefits:

- Faster access to logging information due to smaller log files.
- Improved administration of log records through regular change-overs and back-ups of the offline log files.
- Possibility of performing extensive searches in the offline logging information without affecting ongoing openFT operation.

Saving and deleting log records

As one of your duties as FT administrator, you should regularly create backups of the log records from the current log file or from the offline log file(s) as a file in CSV format or on tape, for example and then delete the log records or offline log file(s) with the DELETE-FT-LOGGING-RECORDS command.

In this way you have a complete, uninterrupted log at your disposal for documentation purposes, while at the same time no storage capacity is wasted. Bear in mind the assigned file size of the current log file does not change when you delete log records, but the space formerly occupied by the records you delete is released within the file.

Viewing the contents of a log record

The information content of the FT logging records includes:

- date and time of request processing,
- an acknowledgment indicating correct completion of a request, or the reason for request rejection or abort,
- the direction of file transfer,
- the name of the partner system involved in file transfer.
- TSN and user ID of the request initiator for requests submitted in the local system; only *REMOTE is entered for remote request initiators,
- the user ID under which the request was handled or should have been handled,
- the name of the file.
- the global request ID for inbound requests
- if an abort occurs, additional information on the cause.

The FT administrator can use the SHOW-FT-LOGGING-RECORDS command to output all FT logging records of his/her system to SYSOUT or SYSLST. Two formats are available for the output: a format that is suitable for listings, and a CSV format that is optimized for further processing. He/she can also choose between a brief overview or a long detailed output and use NUMBER=*POLLING(..) to repeat the output of the new log records at regular intervals.

If the FTAC functionality is being used, the logging records relevant for FTAC are saved in the same file. A detailed description of the command SHOW-FT-LOGGING-RECORDS can be found on page 315ff; the output is presented starting on page 326.

Modifying logging settings

You can set the scope of the logging functions and define the times and intervals for the automatic deletion of log records.

Setting the scope of logging

You set the scope of logging with the LOGGING=SELECT(...) operand in the MODIFY-FT-OPTIONS command.

You can set the scope of FT, FTAC and administration function logging differently. Following installation, full logging is set.

Setting the automatic deletion of log records

You can set the intervals for the automatic deletion of log records in the MODIFY-FT-OPTIONS command by setting the operand DELETE-LOGGING=*PAR(..). This setting deletes log records as of a defined minimum age at regular intervals and at a specified time. This automatic delete function is only active if openFT is started. If openFT is not started at a scheduled delete time then the delete operation is not performed on the next start-up.

Following installation, the automatic deletion of log records is disabled. You should only enable this function if you do not require the uninterrupted recording of log records.

3.6.2 Console messages for automatic monitoring

Messages are usually issued as responses to administration commands. There are, however, also some messages which are not (or not exclusively) issued by administration commands. These messages can be consulted on the manual server (*http://manuals.ts.fujitsu.com*) using an HTML application. ”. When errors occur on accessing the request queue or the partner list, openFT generates normal DMS error messages.

To support automatic monitoring, some events which are not direct responses to user input are reported by openFT via a console message. Depending on which events are involved, further actions can then be initiated by automatic operators such as Omnis-Prop, HLL-Prop, etc. Console messages can also be used to generate SNMP traps for automatic FT monitoring using SNMP.

The console messages for automatic monitoring occupy the message code range from FTR0300 to FTR0399. They have the routing code ‘@’, which means that they must be explicitly requested, for example, using the following command

```
/MOD-MSG-SUBSCRIPTION ADD-MSG-ID=(FTR0301,FTR0307,FTR0340,FTR0341)
```

Messages for monitoring partner systems

FTR0301 Partner '(&00)' entered state NOCON

FTR0302 Partner '(&00)' entered state ACTIVE

FTR0303 Partner '(&00)' entered state LUNK

FTR0304 Partner '(&00)' entered state RUNK

FTR0305 Partner '(&00)' entered state INACTIVE

FTR0306 Partner '(&00)' entered state AINAC

FTR0307 Partner '(&00)' may be unreachable

FTR0308 Partner '(&00)' does not allow any more inbound requests

FTR0309 Partner '(&00)' added

FTR0310 Partner '(&00)' removed

FTR0311 Partner '(&00)') entered state LAUTH

FTR0312 Partner '(&00)' entered state RAUTH

FTR0313 Partner '(&00)' entered state DIERR

FTR0314 Partner '(&00)' entered state NOKEY

FTR0315 Partner '(&00)' entered state IDREJ

Messages for monitoring openFT

FTR0320 abnormal termination initiated

FTR0360 openFT control process started

FTR0361 openFT control process terminated

Messages for monitoring the request queue

FTR0330 Request queue 85 percent full

FTR0331 At least 20 percent of request queue unoccupied

Messages for monitoring requests

FTR0340 Transfer '(&00)' successfully completed

FTR0341 Transfer '(&00)' terminated with error

3.6.3 Monitoring openFT using a job variable

You can monitor an openFT instance by an automatically populated MONJV. The job variable is located under the configuration user ID of the instance concerned (e.g. $SYSFJAM) and has the name MONJV.OPENFT. The content of the job variable complies with the standard for MONJVs. The following information is provided by openFT:

Position 1-2 = state:

$R	open FT is active.
$T	openFT has been terminated normally.
$A	openFT has been terminated abnormally.

Position 5-8 = TSN of the control process of the instance involved.

The job variable is created the first time START-FT is issued and used thereafter. If it is not possible to modify the job variable for some reason, this does not have any effect on openFT operation. A diagnostics record is simply created in order to subsequently identify the cause.

3.6.4 SNMP management for openFT

SNMP stands for **S**imple **N**etwork **M**anagement **P**rotocol and was developed as the protocol for network management services in TCP/IP networks. openFT permits you to centrally monitor and administer one or more openFT systems from one central management station using graphical interfaces. A prerequisite for SNMP-based openFT management is the installation of the products SNMP Management ≥ V6.0, SNMP Basic Agent BS2000 V6.0 (SBA-BS2) and SNMP Standard Collection BS2000 V6.0 (SSC-BS2).

Detailed information can be found in the respective user manuals.

To support automatic monitoring, some events which are not direct responses to user input are reported by openFT via a console message. Console messages can also be used to generate SNMP traps for automatic FT monitoring using SNMP.

If the file transfer subagent is used then openFT itself can also generate SNMP traps (without having to use console messages).

The file transfer subagent is used to:

- start and stop openFT for BS2000
- acquire system parameter information
- change the public key for encryption
- output statistics
- diagnostic control
- output partner information

The proprietary MIB for openFT contains objects for the management tasks listed above. The objects for starting and stopping, changing the public key for encryption, and for diagnostic control also provide write access.

3.6.4.1 Starting and stopping openFT

MIB definition/ object identifier	Access	Meaning
ftStartandStop 1.3.6.1.4.1.231.2.18.1.1.0	read-write	Start / Stop

openFT is started and stopped via the openFT subagents by setting the value “START” or “STOP” respectively. A read access returns information on the current FT system state.

3.6.4.2 System parameters

MIB definition/ object identifier	Access	Meaning
ftSysparVersion/ 1.3.6.1.4.1.231.2.18.2.1.0	read-only	Version
ftSysparTransportUnitSize/ 1.3.6.1.4.1.231.2.18.2.2.0	read-write	Transport Unit Size
ftSysparTaskLimit/ 1.3.6.1.4.1.231.2.18.2.3.0	read-write	Task Limit
ftSysparConnectionLimit/ 1.3.6.1.4.1.231.2.18.2.4.0	read-write	Connection Limit: maximum number of transport connections that can be reserved for the execution of FT requests
ftSysparPartnerCheck/ 1.3.6.1.4.1.231.2.18.2.6.0	read-write	Partner Check
ftSysparMaxInboundReqs/ 1.3.6.1.4.1.231.2.18.2.12.0	read-write	Max Inbound Requests: maximum number of inbound requests per partner system
ftSysparMaxLifeTime/ 1.3.6.1.4.1.231.2.18.2.13.0	read-write	Max Request Lifetime: maximum lifetime (in days) in the request queue

Further information of the output values can be found in the section on the SHOW-FT-OPTIONS command on page 351.

3.6.4.3 Public key for encryption

MIB definition/ object identifier	Access	Meaning
ftEncryptKey/ 1.3.6.1.4.1.231.2.18.3.1.0	write-only	An entry of “create-new-key” or “1” causes a new public key to be generated.

3.6.4.4 Statistics

MIB definition/ object identifier	Access	Meaning
ftStatSuspend/ 1.3.6.1.4.1.231.2.18.4.1.0	read-only	Requests in a SUSPEND state
ftStatLocked/ 1.3.6.1.4.1.231.2.18.4.2.0	read-only	Requests in a LOCKED state
ftStatWait/ 1.3.6.1.4.1.231.2.18.4.3.0	read-only	Requests in a WAIT state
ftStatActive/ 1.3.6.1.4.1.231.2.18.4.4.0	read-only	Requests in an ACTIVE state
ftStatCanceled/ 1.3.6.1.4.1.231.2.18.4.5.0	read-only	Requests in a CANCELD state
ftStatFinished/ 1.3.6.1.4.1.231.2.18.4.6.0	read-only	Requests in a FINISHED state
ftStatHold/ 1.3.6.1.4.1.231.2.18.4.7.0	read-only	Requests in a HOLD state
ftStatLocalReqs/ 1.3.6.1.4.1.231.2.18.4.8.0	read-only	Async requests in the local system
ftStatRemoteReqs/ 1.3.6.1.4.1.231.2.18.4.9.0	read-only	Requests in the remote system

A description of the output values can be found in the section on the SHOW-FILE-TRANSFER command on page 284.

3.6.4.5 Diagnostic control

MIB definition/ object identifier	Access	Meaning
ftDiagStatus/ 1.3.6.1.4.1.231.2.18.5.1.0	read-write	on / off
ftDiagFtamPartners/ 1.3.6.1.4.1.231.2.18.5.2.0	read-write	on / off
ftDiagOpenftPartners/ 1.3.6.1.4.1.231.2.18.5.3.0	read-write	on / off
ftDiagFtpPartners/ 1.3.6.1.4.1.231.2.18.5.4.0	read-write	on / off
ftDiagSynRequests/ 1.3.6.1.4.1.231.2.18.5.5.0	read-write	on / off
ftDiagAsynRequests/ 1.3.6.1.4.1.231.2.18.5.6.0	read-write	on / off
ftDiagLocRequests/ 1.3.6.1.4.1.231.2.18.5.7.0	read-write	on / off
ftDiagRemRequests/ 1.3.6.1.4.1.231.2.18.5.8.0	read-write	on / off
ftDiagOptionsNobulk/ 1.3.6.1.4.1.231.2.18.5.9.0	read-write	on / off

Please also read the section on the MODIFY-FT-OPTIONS command on page 223.

3.6.4.6 Partner Information

MIB definition/ object identifier	Access	Meaning
ftPartnerName/ 1.3.6.1.4.1.231.2.18.8.1.1.1.0	read-only	Name of the FT partner
ftPartnerType/ 1.3.6.1.4.1.231.2.18.8.1.1.2.0	read-only	FT protocol used by the partner
ftPartnerState/ 1.3.6.1.4.1.231.2.18.8.1.1.3.0	read-write	Status of the FT partner: act (1), inact (2), nocon (3), lunk (4), runk (5), adeact (6), ainact (7) lauth (8) rauth (9) dierr (10) nokey (11) idrej (12)
ftPartnerAddress/ 1.3.6.1.4.1.231.2.18.8.1.1.10.0	read-only	Address of the partner system

Only a status update for one partner is supported at present, and only the values act, inact and adeact may be specified.

3.6.4.7 Traps

Object name/ object identifier	Trap No.	Explanation
Enterprise = sniFTTraps		
ftStopTrap/ 1.3.6.1.4.1.231.2.18.6.0.1.0	1	TRAP is sent if openFT is terminated
ftPartnerStateTrap/ 1.3.6.1.4.1.231.2.18.6.0.4.0	4	TRAP is sent if the partner status has changed
ftPartnerUnreachableTrap/ 1.3.6.1.4.1.231.2.18.6.0.5.0	5	May not be possible to access partner
ftStartTrap/ 1.3.6.1.4.1.231.2.18.6.0.6.0	6	TRAP is sent after start of openFT
ftRequestQueueUpperLimitTrap/ 1.3.6.1.4.1.231.2.18.6.0.7.0	7	TRAP is sent if the FT request queue is more than 85% full
ftRequestQueueLowerLimitTrap/ 1.3.6.1.4.1.231.2.18.6.0.8.0	8	TRAP is sent if at least 20% of the FT request queue is free again
ftRequestSuccessfulTrap/ 1.3.6.1.4.1.231.2.18.6.0.9.0	9	TRAP is sent if an FT request is sent successfully
ftRequestErrorTrap/ 1.3.6.1.4.1.231.2.18.6.0.10.0	10	TRAP is sent if an FT request is terminated with an error
ftSubsystemStartTrap/ 1.3.6.1.4.1.231.2.18.6.0.11.0	11	TRAP is sent if the FT subsystem has been started
ftSubsystemStopTrap/ 1.3.6.1.4.1.231.2.18.6.0.12.0	12	TRAP is sent if the FT subsystem has been stopped

3.6.4.8 Trap groups and trap controls

The traps of the openFT subagent can be gathered together into groups that are represented by the following MIB objects. This means that you can enable or disable the sending of traps for the individual trap groups as follows (trap send status “on” or “off”):

– Specification 2 (“on”): the traps for the group in question are sent.

– Specification 1 (“off”): the traps for the group in question are not sent.

MIB definition/ object identifier	**Access**	**Affected traps**
ftTrapsSubsystemState/ 1.3.6.1.4.1.231.2.18.10.1.0	read-write	– ftSubsystemStartTrap – ftSubsystemStopTrap
ftTrapsFTState/ 1.3.6.1.4.1.231.2.18.10.2.0	read-write	– ftStartTrap – ftStopTrap
ftTrapsPartState 1.3.6.1.4.1.231.2.18.10.3.0	read-write	– ftPartnerStateTrap
ftTrapsPartnerUnreachable/ 1.3.6.1.4.1.231.2.18.10.4.0	read-write	– ftPartnerUnreachableTrap
ftTrapsRequestQueueState/ 1.3.6.1.4.1.231.2.18.10.5.0	read-write	– ftRequestQueueUpperLimitTrap – ftRequestQueueLowerLimitTrap
ftTrapsTransSucc/ 1.3.6.1.4.1.231.2.18.10.6.0	read-write	– ftRequestSuccessfulTrap
ftTrapsTransFail/ 1.3.6.1.4.1.231.2.18.10.7.0	read-write	– ftRequestErrorTrap

3.6.4.9 Trap information

The MIB of the openFT subagent contains definitions of MIB objects which are sent together with the traps.

MIB definition/ object identifier	**Access**	**Explanation**
ftRequestID/ 1.3.6.1.4.1.231.2.18.9.1.0	not-accessible	Transfer ID of the request
ftRequestInitiator/ 1.3.6.1.4.1.231.2.18.9.2.0	not-accessible	Initiator of the request: local (1), remote (2)
ftRequestPartnerName/ 1.3.6.1.4.1.231.2.18.9.3.0	not-accessible	Partner
ftRequestUserID/ 1.3.6.1.4.1.231.2.18.9.4.0	not-accessible	User ID of submitter
ftRequestFileName/ 1.3.6.1.4.1.231.2.18.9.5.0	not-accessible	Name of the file for transfer
ftRequestError/ 1.3.6.1.4.1.231.2.18.9.6.0	not-accessible	Error in request

3.6.5 Monitoring with openFT

openFT provides the option of monitoring and recording a range of characteristic data for openFT operation. The data falls into three categories:

- Throughput, e.g. total network throughput caused by openFT
- Duration, e.g. processing time for asynchronous jobs
- State, e.g. number of requests currently queued

You must be an FT administrator in order to activate, deactivate or configure monitoring.

As soon as monitoring is activated, any user can call up the data and output it based on certain criteria.

3.6.5.1 Configuring monitoring

You configure monitoring using the MODIFY-FT-OPTIONS command and the MONITORING= operand (see page 223). The following options are available:

- Activating and deactivating monitoring
- Selective monitoring based on the partner type
- Selective monitoring based on the request type

Once you have chosen your settings, they are retained until you change them explicitly. This means that they are also not changed if you reboot the computer.

You can check the current settings with SHOW-FT-OPTIONS. The MONITOR row indicates whether monitoring is activated and shows any criteria used for selection.

3.6.5.2 Showing monitoring data

If monitoring is activated. the monitoring data can be called up on the local system or from a remote system.

Outputting monitoring data on the local system

Use the command SHOW-FT-MONITOR-VALUES to show monitoring data locally (see page 337).

SHOW-FT-MONITOR-VALUES outputs the monitoring data in the form of tables that you can further process as required either programmatically or using an editor.

When you call SHOW-FT-MONITOR-VALUES, you can select specific monitoring data for output, whether or not output is formatted and the time interval at which output is performed. You can also specify the output medium. You can find details on the values output on page 343.

Showing monitoring data on remote Unix or Windows systems

The monitoring data can also be shown in the openFT Monitor on a remote Unix or Windows system. To do this, you set up a special admission profile that is specified when the openFT monitor is called and causes only the monitoring values to be read and transferred. The admission profile uses the keyword *FTMONITOR as a preprocessing command and is set up as follows:

```
/CREATE-FT-PROFILE NAME=MONITOR,TRANSFER-ADMISSION=ONLYFTMONITOR -
       ,FILE-NAME=*EXPANSION('|*FTMONITOR ') -
       ,FT-FUNCTION=(*TRANSFER-FILE,*FILE-PROCESSING)
```

ONLYFTMONITOR is the (freely selectable) FTAC transfer admission that must be specified when the openFT Monitor is called. Alternatively, this transfer admission can also be specified in an ft or ncopy command used to transfer monitoring data in a Unix or Windows system.

You will find details in the openFT manuals "openFT V12.0 for Unix Systems - Installation and Administration" and "openFT V12.0 for Windows Systems - Installation and Administration".

3.7 Administrating and controlling FTAC functions

FTAC provides the functions for controlling FT activities on a computer-specific and user-specific basis using admission sets and admission profiles..

The admission set for a particular user ID defines which FT functions the user ID may use and for which *partner systems*.

Admission profiles define a transfer admission that has to be specified in FT requests instead of the LOGON or Login authorization. The admission profile defines the access rights for a user ID by restricting the use of parameters in FT requests.

The FT administrator must assign security levels to the partner systems (see ADD-FT-PARTNER and MODIFY-FT-PARTNER SECURITY-LEVEL operand and section "FTAC security levels for partners in the partner list" on page 48).

The security level of a partner entry is taken into account when a user wants to process a request via this partner entry. FTAC compares the security level of the partner entry with the security level for this function (e.g. inbound sending) specified in the user's admission set. If the security level in the admission set is lower than that in the partner entry, the request is rejected by FTAC. If a privileged FTAC profile is used for the request, it can override the restrictions defined in the admission set.

As FTAC administrator, you can use SHOW-FT-RANGE to list all the partner systems with which your FT system can communicate via file transfer. In addition, you can display which partner systems can be accessed from any user ID in the system.

WARNING!

Note that openFT-AC is only effective for connected products such as openFT. If other file transfer products without an openFT-AC connection are also being used, a more comprehensive and coordinated security concept would be advisable.

3.7.1 Creating a default admission set

The FTAC administrator must first determine an average protection level for the user IDs in his system and use this information to modify the default admission set, whose values after the installation of openFT-AC are all 0. In the default admission set, the settings are made for the "average" FTAC user in the system. This provides adequate protection for most users. These specifications are valid for all user IDs which do not have their own admission set. Furthermore, in each admission set, the entry *STD can be used in different places to refer to the default admission set. This has the advantage of automatically incorporating any modification of the default admission set into these admission sets.

The FTAC administrator can set individual values for user IDs whose protection requirements deviate from the average.

3.7.2 Administrating admission sets

For the administration of admission sets, openFT-AC offers the FTAC administrator the following commands:

MODIFY-FT-ADMISSION-SET	Modify admission sets
SHOW-FT-ADMISSION-SET	Show admission sets

A maximum security level is specified in the admission set for each of the six basic functions (inbound send, inbound receive, inbound follow-up processing, inbound file management, outbound send, outbound receive). The user ID with this admission set can use this basic function with all partner systems who have this security level or lower.

The FTAC administrator modifies the admission sets with the command MODIFY-FT-ADMISSION-SET (see page 213).This command is used to modify the default admission set as well as to customize the settings for individual user IDs. The specifications of the FTAC administrator are the maximal security levels in the admission set for the corresponding user ID. The user can increase the degree of protection within these levels i.e. define even stricter security levels. You can display the admission sets using the SHOW-FT-ADMISSION-SET command (see page 306). The command displays both the levels predefined by the administrator (MAX-ADM-LEVELS) and the levels set by the user (MAX-USER-LEVELS)..

With an openFT request (outbound and inbound), the admission is compared with the FTAC security level of the partner concerned (see also page 48).

3.7.3 Administrating admission profiles

For the administration of admission profiles, openFT-AC offers the FTAC administrator the following commands:

CREATE-FT-PROFILE	create admission profile
DELETE-FT-PROFILE	delete admission profile
MODIFY-FT-PROFILE	modify admission profile
SHOW-FT-PROFILE	show admission profile

The FTAC administrator has the option of modifying foreign admission profiles:

- He can view them with the command SHOW-FT-PROFILE (see page 372). The transfer admission of an admission profile is not output. This means that the FTAC administrator does not have access rights to the files of foreign user IDs.
- He can delete them with the command DELETE-FT-PROFILE (see page 187). This is the most radical of all options which should only be used in extreme cases and with good reason and upon consultation with the owner of the profile.
- He can privilege them with the command MODIFY-FT-PROFILE (see page 257), or conversely revoke privileges.
- He can also modify them with MODIFY-FT-PROFILE. Access to the admission profile will then be blocked until the owner of the profile acknowledges these modifications by resetting the transfer admission to “valid”, for example with MODIFY-FT-PROFILE <profile> TRANSFER-ADMISSION=*OLD-ADMISSION(VALID=*YES). If the FTAC administrator also possesses the TSOS privilege or specifies explicitly the account and the password in the profile, then the profiles are not locked.

Privileging admission profiles

In exceptional cases, the FT user can use a privileged admission profile to disregard the specifications of own admission profile. The user ID protection is maintained in this case, by the fact that only very restricted access is permitted into the admission profile. Exceptional cases where this is allowed include:

- if a particular file needs to be transferred,
- if follow-up processing is not permitted or severely restricted,
- if a partner system with a higher security level is permitted to carry out file transfers with the user ID, but others with lower security levels are not.

The procedure to follow when privileging an admission profile is simple:

1. The user creates an admission profile for the planned task with the command CREATE-FT-PROFILE.
2. The FTAC administrator views the admission profile with the command SHOW-FT-PROFILE to determine if the profile presents a threat to data security.

   Example

   ```
   /SHOW-FT-PROFILE NAME=PROFPROD,
                    SELECT-PARAMETER=(OWNER-IDENTIFICATION=STEVEN),
                    INFORMATION=*ALL
   ```

   Short form:

   ```
   /SHOW-FT-PROF PROFPROD,SEL=(,STEVEN),INF=*ALL
   ```

   The output has the following form:

   ```
   %PROFPROD
   % IGN-MAX-LEV = (IBR)
   % FILE-NAME   = PROFIT
   % USER-ADM    = (STEVEN,M4711DON,OWN)
   % PROC-ADM    = SAME
   % FT-FUNCTION = (TRANSFER-FILE, MODIFY-FILE-ATTRIBUTES,
                    READ-FILE-DIRECTORY)
   % LAST-MODIF  = 2012-06-13 08:24:49
   ```

   The first line of the output shows the name of the admission profile, the second line the values which STEVEN has set in the command CREATE-FT-PROFILE (page 157) or which are determined by the default values, if Steven doesn't set them himself.

3. If the profile will not endanger security, the FTAC administrator privileges it with the help of the command MODIFY-FT-PROFILE.

   Example

   ```
   /MODIFY-FT-PROFILE NAME=PROFPROD,
                      SELECT-PARAMETER=(OWNER-IDENTIFICATION=STEVEN),
                      PRIVILEGED=*YES
   ```

In a privileged admission profile, only the transfer admission and the parameter PRIVILEGED may be modified by the user. This prevents the misuse of any profiles, once privileged.

3.7.4 Transfer FTAC environment - the environment functions

The following commands are available for the environment functions:

EXPORT-FTAC-ENVIRONMENT	output FTAC environment to file
IMPORT-FTAC-ENVIRONMENT	transfer FTAC environment from file
SHOW-FTAC-ENVIRONMENT	show FTAC environment from export file

The FTAC administrator can have admission profiles and sets written (i.e. “exported”) to a file and thus back up all admission profiles and sets that exist on the computer. In addition, this function is useful when a user migrates from one computer to another. In this case, the FTAC administrator first backs up the existing FTAC environment to a file and then re-installs this on another computer. The FTAC user can then continue to work in the same FTAC environment as before, i.e. with the same admission profiles and the same admission set.
Any existing privileges must be explicitly set up again on the new computer, and the admission profiles must be explicitly released if the FTAC administrator does not possess the TSOS privilege.
On the other hand, if the FTAC administrator has the TSOS privilege, he/she can specify on importing whether the profiles will be imported with unmodified attributes or not.

The FTAC administrator can also selectively back up (EXPORT-FTAC-ENVIRONMENT, page 199) admission sets and profiles by using corresponding parameter specifications and then restore them when needed (IMPORT-FTAC-ENVIRONMENT, page 201). This can be done with:

– admission profiles and admission sets of one or more users (up to 100)
– all admission profiles and admission sets on a given computer
– only admission sets, no admission profiles
– only admission profiles, no admission sets

The contents of a backup file can be viewed with the command:

SHOW-FTAC-ENVIRONMENT

which displays the FTAC environment from the export file (see page 302).

Example

Steven Miller needs to work on a new computer under the same user ID STEVEN. Steven would like to keep the same admission set and admission profiles as before. To do this, the FTAC administrator Jack backs up the admission set and the admission profiles for the user ID STEVEN in the file STEVEN.FTAC.BKUP.

```
/EXPORT-FTAC-ENVIRONMENT TO-FILE=STEVEN.FTAC.BKUP,
                         USER-IDENTIFICATION=STEVEN
```

Being a conscientious FTAC administrator, Jack John checks if the desired backup is in the file STEVEN.FTAC.BKUP.

```
/SHOW-FTAC-ENVIRONMENT FROM-FILE=STEVEN.FTAC.BKUP
```

He receives the following output:

```
                MAX. USER LEVELS               MAX. ADM LEVELS          ATTR
% USER-ID  OBS  OBR  IBS  IBR  IBP  IBF   OBS  OBR  IBS  IBR  IBP  IBF
% STEVEN     1    1    0    1    0    0     1    1    0    0    0    0
% OWNER     NAME
% STEVEN   *PROFPROD
```

Now, Jack transfers the file STEVEN.FTAC.BKUP to the user ID of the FTAC administrator on the new computer.
There, Sylvester the Cat, the FTAC administrator for the new computer, transfers the admission set and the admission profiles of the user ID STEVEN from the file STEVEN.FTAC.BKUP.

Sylvester is also a conscientious administrator. He checks if Steven’s admission sets and profiles are a threat to the security of his system (he doesn’t trust Jack in the slightest):

```
/SHOW-FTAC-ENVIRONMENT FROM-FILE=STEVEN.FTAC.BKUP
```

and of course he receives the same output as above.

Then Sylvester imports Steven’s admissions from the file STEVEN.FTAC.BKUP onto his system:

```
/IMPORT-FTAC-ENVIRONMENT FROM-FILE=STEVEN.FTAC.BKUP
```

Since Sylvester the Cat does not possess the TSOS privilege, he must now privilege Steven’s profile:

```
/MOD-FT-PRO UMSAWARE,,(,STEVEN),PRIV=*Y
```

Finally, Steven must release the imported profiles before he can work with them. This would not be necessary if Sylvester the Cat possessed the TSOS privilege.

```
/MODIFY-FT-PROFILE NAME=*ALL,
                   TRANSFER-ADMISSION=*OLD(VALID=*YES)
```

3.7.5 The FTAC logging function

openFT-AC checks the access rights of every FT request which the protected system is involved in and logs the results. This information is stored in the so-called FTAC logging records.
The following information can be called up by the FTAC administrator:

- logging date
- type of logging record (FT or FTAC logging record)
- logging number of the FT request
- time of access check
- code for the function of the FT request (see table)
- reason for any rejections of the request by FTAC (the User Guide contains an overview of the codes for these reasons)
- transfer direction of the FT request
- name of the partner system with which the FT request was/is to be carried out
- TSN process sequential number and USER-IDENTIFICATION LOGON authorization of the initiator of requests which were made in the local system (or *REMOTE for remote request initiators)
- name and privileging identifier of any admission profiles used
- the local file or library name

FTAC only checks the admission for a request on the basis of the admission sets and admission profiles. openFT logs whether or not it can actually execute the request in the FT or ADM log records. For further details, see section “SHOW-FT-LOGGING-RECORDS Display log records and offline log files” on page 315.

The display of FTAC logging records can not be turned off. However, the MODIFY-FT-OPTIONS command can be used to restrict it to requests rejected by FTAC (*REJECTED) or to modified requests (*MODIFICATIONS).

The FT command SHOW-FT-LOGGING-RECORDS can be used by the FTAC administrator to find out about all access checks which have been carried out by openFT-AC to date (see page 315). This facilitates processes such as system inspections.

Codes for the function of the FT request

The entries in front of the brackets indicate the log representations of the individual FT functions. The FT requests themselves can consist of groups of FT functions. However, only one will appear in the logging record. These groups are listed in the brackets.

␣	TRANSFER-FILE	(WRITE-FILE + ... or READ-FILE + ...)
A	READ-FILE-ATTRIBUTES	(READ-FILE-ATTRIBUTES + ...)
D	DELETE-FILE	(DELETE-FILE + ...)
C	CREATE-FILE	(CREATE-FILE + ...)
M	MODIFY-FILE-ATTRIBUTES	(MODIFY-FILE-ATTRIBUTES + ...)
R	READ-DIR	(READ-DIR + ...)
CD	CREATE-DIR	
MD	MODIFY-DIR	
DD	DELETE-DIR	
L	FTP-LOGIN [1]	

[1] Is generated on failed access attempts via openFT-FTP

To make the output of the command SHOW-FT-LOGGING-RECORDS provide more of an overview, you can specify values or value ranges for various output parameters when calling up the command. This permits you to be selective in the output of logging records.

Deleting logging records

The FT administrator and the FTAC administrator are the only users in the system who can not only view but also delete the FTAC logging records. The corresponding FT command is DELETE-FT-LOGGING-RECORDS (see page 182). The FT user can view only his own log records, he may not delete log records.

FTAC logging records can only be deleted from the oldest date up to a specified date. This ensures that there will be no gaps in the log file up to the most current record.

In theory, openFT-AC can write any number of logging records (“until the disk is full”). From time to time, the FTAC administrator should make a backup of existing logging records (either print out a hard copy or make a copy on tape or save a file in CSV format) and then delete these logging records from the log file. This ensures that the logging records will provide a continuous record over an extended period of time, as well as prevent the log file from getting too large. As of openFT V12, you can change the current log file and retain older log records in offline log files (see page 66).

3.8 Using openFT in a HIPLEX cluster

In openFT you can run multiple openFT instances on one computer simultaneously. Because of these instances, should a computer fail, you are in a position to carry over the functionality of the openFT to another computer, which is already running openFT.

After installing openFT, the **default instance** exists on each computer. This instance is atypical in that it cannot be deleted by instance management commands. Its application data is located on the default pubset under ID $SYSFJAM. When instances are displayed (SHOW-FT-INSTANCE), the default instance is always displayed first.

Up to 16 additional instances can be created by administration. Each of these instances, including the standard instance, consists of the following components:

- The request file SYSRQF, the partner list SYSPTF, the logging file SYSLOG, trace files, options SYSOPF and the profile file SYSFSA. Each instance therefore requires a configuration user ID with the characteristics that are described for the SYSFJAM ID (see section “Preparing the FT system” on page 25).
  Exception: It is not necessary that the configuration user ID is located on the home pubset.
- Each instance requires its own network address; this always remains the same, independent of the real host. The host name must therefore be stored in the options using the MODIFY-FT-OPTIONS command. This (virtual) BCAM host must always be accessible under the same network address. In order to prevent the BCAM connection setup from automatically being passed to the real host instance when an instance fails to start, BCAM aliasing should be disabled for the $FJAM and $FTAM applications.

The openFT installation files are only available once per computer and are shared by all the instances. The same version, however, must be installed on all the computers in the cluster (openFT version, proofing version, reps, etc.).

openFT commands that are called during a preprocessing, postprocessing or follow-up processing session, run under the same instance as the request that initiated the processing.

Commands for administrating openFT instances

As the openFT administrator, you can create, modify, and delete instances. In addition, you can set and get information on instances (like a user). The creation, modification and deletion of instances is only possible via the SDF interface, not via the POSIX command interface.

- Creating an instance

  Using the CREATE-FT-INSTANCE command, you can create an instance.

  If an instance is created, an entry is made in the administration file. This entry consists of the name of the instance and the pubset and user ID in which the files required for operation are stored (the request file, partner list, etc.). All the initialization tasks are carried out in the same way as during START-SUBSYSTEM. In the event you have also specified the AUTOMATIC-START option, then openFT is subsequently and immediately started in this instance.

- Modifying an instance

  With the MODIFY-FT-INSTANCE command, you can rename an instance and modify its AUTOMATIC-START characteristics.

- Deleting an instance

  With the DELETE-FT-INSTANCE command, you can delete an instance. Deleting an instance removes the administration entry for the instance. All the variable data (the request file, partner list, etc.) of this instance continue to exist and can be re-activated by repeating the CREATE-FT-INSTANCE command. Any attempt to access a deleted instance is denied with FTR0236.

  The default instance cannot be deleted.

- Setting an instance

  Using the SET-FT-INSTANCE command, you can select the openFT instance with which you would like to work (see the user guide). This setting is then valid for all the SDF commands set under this task or program interface calls and remains valid until the task is ended or until the next SET-FT-INSTANCE command. If you want to continue to work with the set instance in a Posix shell then it is necessary to call the following command after starting the shell:

  ```
  . ftseti
  ```

  The dot (.) followed be a blank is mandatory!

  It is therefore advisable to record this command in the */etc/profile* file.
  If no SET-FT-INSTANCE command is given in a task, then work proceeds using the default instance.

- Displaying instance information

  Using the SHOW-FT-INSTANCE command, you can request information regarding the instances, see the user guide.

- Set or display the BCAM host

  Using the MODIFY-FT-OPTIONS ...,HOST-NAME command, you can assign the current instance a BCAM host. This BCAM host will be used for communication of openFT. By doing this, an instance allows itself to be assigned a fixed transport address, which is independent of the computer on which the instance is running.

  On executing the SHOW-FT-OPTIONS command, the name of the BCAM host with which the instance is working is displayed.

- Importing an instance to another computer

  The following steps are required to change over an openFT instance to another computer:

  - Stop the instance on the original computer (/STOP-FT).
  - Unload the instance on the original computer (/DELETE-FT-INSTANCE). This unlocks all of the files required by openFT (request file, transfer files, etc.).
  - Import the variable files, the network address (virtual BCAM host) and all of the files required by the requests to the destination computer. This can contain, among other things, the switching over of one or several pubsets).

    It is recommended to import all files of the configuration user ID when changing over.
  - Load the instance on the destination computer (/CREATE-FT-INSTANCE).
  - Start the instance on the destination computer (if this does not occur automatically, then use /SET-FT-INSTANCE, /START-FT).

  After importing an instance to another computer, openFT finishes the (under some circumstances restartable) requests, whose admissions were already checked before importing. The new environment must have the same prerequisites as the old computer (the same IDs with the same file access admissions).

  All pubsets that are accessed by requests must be available. All requests whose pubsets are not accessible during restart attempts are aborted.

  On the new computer, the network view must be the same as that on the old computer. This means that, from the point of view of the BCAM, the same host names for partner computers must be available and they must refer to the same partner computer. The network address of the (virtual) host on which the instance is running, must be seen from the outside the same as from the address of the host, on which the instance was previously running.

  The name of the instance must be the same on all of the computers, since, for example, it is used for qualifying temporary files.

3.9 Diagnostics

3.9.1 Controlling the trace function

The FT administrator uses the following commands to control the trace function:

ADD-FT-PARTNER	Add a remote system to the partner list
MODIFY-FT-OPTIONS	Modify partner characteristics
MODIFY-FT-PARTNER	Information about operating parameters

The FT administrator uses the following commands to get information on the current settings:

SHOW-FT-OPTIONS	Information about operating parameters
SHOW-FT-PARTNERS	Information about partner systems

The FT trace function can be switched on and off irrespective of whether the FT system is active or inactive.

You can set the scope of openFT traces globally using the MODIFY-FT-OPTIONS command. You can differentiate by partner type (openFT, FTP, FTAM), request type (local/remote and synchronous/asynchronous) and trace scope (with/without file contents). The global setting can be modified on a partner-specific basis using MODIFY-FT-PARTNER (or set before with ADD-FT-PARTNER).
The following table illustrates four typical cases of trace use.

MODIFY-FT-OPTIONS	**ADD-/MODIFY-FT-PARTNER**	**Task**	**Effect**
TRACE=*ON	TRACE= *BY-FT-OPTIONS	General tracing of FT operations.	FT operation is fully traced.
TRACE=(SWITCH=ON, OPTIONS= NO-BULK-DATA)	TRACE= *BY-FT-OPTIONS	Connect tracing for all openFT partners.	Mass data transfers are not recorded. Recommended for long-lived traces.
TRACE=(SWITCH=ON ,PART-SELECTION= *FTP)	TRACE= *BY-FT-OPTIONS	Tracing of a a certain type of partner over an extended period. (here, ftp partners)	All events relating to a selected partner type are logged. Despite the extended period, the trace volume does not become excessive.

MODIFY-FT-OPTIONS	**ADD-/MODIFY-FT-PARTNER**	**Task**	**Effect**
TRACE=(SWITCH=ON ,REQ-SELECTION= *REM)	TRACE= *BY-FT-OPTIONS	Tracing of a specific type of request (here, requests submitted by a remote system)	All events relating to certain request types are logged. Despite the extended period, the trace volume does not become excessive.

The default value for ADD-FT-PARTNER is BY-FT-OPTIONS. The global settings are thus taken over from MODIFY-FT-OPTIONS.

The following table indicates the interrelations between the most important MODIFY-FT-OPTIONS and ADD-/MODIFY-FT-PARTNER trace settings.

MODIFY-FT-OPTIONS	**ADD-/MODIFY-FT-PARTNER**	**Effect**
TRACE=*OFF	equals	*OFF
TRACE=*ON	TRACE=*BY-FT-OPTIONS	*ON
	TRACE=*UNCHANGED	Setting retained
	TRACE=*ON	*ON
	TRACE=*OFF	*OFF
TRACE=(SWITCH=ON, PARTNER-SELECTION= partner type)	TRACE=*BY-FT-OPTIONS	*ON if suitable partner type *OFF if unsuitable partner type
	TRACE=*UNCHANGED	Setting retained
	TRACE=*ON	*ON
	TRACE=*OFF	*OFF
TRACE=(SWITCH=ON, REQUEST-SELECTION= request type)	TRACE=*BY-FT-OPTIONS	*ON if suitable request type *OFF if unsuitable request type
	TRACE=*UNCHANGED	Setting retained
	TRACE=*ON	as *BY-FT-OPTIONS
	TRACE=*OFF	*OFF

3.9.2 Evaluating traces

openFT generates trace files for the configuration user ID of the openFT instance (default: $SYSFJAM).

Format of the trace files

The file names end with the suffix .FTTF and have the following format:

- Smddhhmm.Sssccc.I000.FTTF'
  Control task.
- Smddhhmm.Sssccc.Iiii.FTTF'
  Server task for inbound and asynchronous outbound requests, i= 001,002, ...
- Ymddhhmm.Sssccc.Pnnnn.FTTF'
  User task for synchronous outbound requests.

mddhhmm.Sssccc specifies the creation time of the trace file. Here, m indicates the month (1 = January, 2 = February, ... A= October, B=November, C = December), dd the day, hhmm the time in hours (hh) and minutes (mm), ssccc the time in seconds (ss) and milliseconds (ccc). nnnn is the TSN of a task for outbound requests.

The trace files contain openFT, FTAM, FTP and ADM requests that have been processed in the corresponding task.

Trace files in the event of errors

- If a trace file cannot be written without errors due to a memory bottleneck, a DLOG record and a console message are output.
- If a record of the trace file cannot be written as a result of an infringement of the maximum record length, the trace file is closed and the subsequent records are written to a new continuation file with the additional suffix.Liii, e.g.:
  S8101010.S33222.I001.FTTF (first trace file)
  S8101010.S33222.I001.L001.FTTF (continuation file)

START-FTTRACE

Traces are evaluated with START-FTTRACE:

START-FTTRACE

INPUT = <filename 1..54>
,**OUTPUT** = <filename 1..54> / *SYSLST
,**TRACE-OPTION** = <c-string 1..50 with-lower-case>
,**SHOW-FILE** = ***NO** / ***YES**
,**PRINT-FILE** = ***NO** / ***YES**

Operand description

INPUT = <filename 1..54>
Filename of the trace file to be evaluated $SYSFJAM.SYSFLF.D*yymmdd*.T*hhmmss.tsn.*

OUTPUT = <filename 1..54>
Filename of the output file.

OUTPUT = *SYSLST
Output to SYSLST, e.g. during preprocessing. This also implicitly sets the SHOW-FILE operand to *NO.

TRACE-OPTION = <c-string 1..50 with-lower-case>
Specifies the options for the trace evaluation in the following format:.

[-d] [-sl=n | sl=l | sl=m | sl=h] [-cxid=<context-id>] [-f=hh:mm:ss] [-t=hh:mm:ss]

-d
Specifies that the trace files are to be output in hexadecimal format (dump format).

CAUTION!
Data that is critical for security (transfer admissions, passwords etc.) is not “masked” in dump format. The specification of a security level or levels is irrelevant here.

-sl=n | **-sl=l** | **-sl=m** | **-sl=h**
Specifies the security level for the output :

n (no) No security requirements, i.e. all the data is output. This includes IDs, passwords, transfer admissions, file names etc.

l (low) Passwords are overwritten with XXX..

m (medium)
Passwords, user IDs, transfer admissions, account numbers and follow-up processing commands are overwritten with XXX. Default value.

h (high)

Passwords, user IDs, transfer admissions, account numbers, follow-up processing commands and file names are overwritten with XXX.
This parameter is not relevant in the case of dump format.

-cxid=<context id>
Selects the trace entries on the basis of the context ID. If you omit *-cxid* or specify *-cxid=* without a context ID then all the trace entries are output.

-f=hh:mm:ss (from)
Specifies the time as of which trace entries in the trace file are to be evaluated. You enter the time in the format hours:minutes:seconds (2 digits each). If you do not specify an end time then trace entries are output up to the end of the file..

-t=hh:mm:ss (to)
Specifies the time up to which trace entries in the trace file are to be evaluated. You enter the time in the format hours:minutes:seconds (2 digits each). If you do not specify an end time then trace entries are output up to the end of the file.

SHOW-FILE =
Specifies if the evaluated trace file should be displayed with the command SHOW-FILE.

SHOW-FILE = *NO
The evaluated trace file is not displayed. Default value in batch mode.

SHOW-FILE = *YES
The evaluated trace file is displayed. Default value in dialog mode.

PRINT-FILE =
Specifies whether the evaluated trace file should be printed.

PRINT-FILE = <u>*NO</u>
The evaluated trace file is not printed.

PRINT-FILE = *YES
The evaluated trace file is printed.

3.9.3 Creating diagnostic records

If, despite due care and attention, an error occurs that neither the FT administrator nor the BS2000 system administrator can rectify, contact your Service Center. To facilitate troubleshooting, please submit the following:

- detailed description of the error situation and statement indicating whether the error is reproducible;
- trace files;
- if applicable the result list of the request that triggered the error;
- SYS.CONSLOG file of the entire session (also from partner system is possible);
- general information as for BS2000 system error on openFT or BS2000/OSD, DCAM, PLAM, SDF and, if required, openFT-FTAM, openFT-AC for BS2000, NFS and POSIX:
  1. system version number,
  2. loader - subversion number / code,
  3. list of all rep corrections used;
- version of the FT partner and details of the transport system (e.g. DCAM, CCP / CMX, VTAM, etc.);
- system dumps requested under the TSN FTxx or FT server tasks;
- system dumps after interrupts in the modules of the FT and FTAC subsystems).

The SHOW-FT-DIAG command can be used to output any diagnostic codes written when the error occurred (together with time and date). In this case, SHOW-FT-DIAG supplies the following output:

```
/SH-FT-DIAG
% DATE          TIME     SSID  COMPONENT    LOCATION-ID      INFO
% 20091021      143307   FT    79/yfasdia   3/EuisyMsg       fd00000c
```

SHOW-FT-DIAG INF=*ALL allows additional information on the current state of openFT to be obtained. This only makes sense, however, if it is done shortly after the problem arises.

3.10 Backing up the configuration data

You should back up the configuration data of your openFT instance at regular intervals. This ensures that you will be able to restore openFT op eration with as little delay as possible using the original runtime environment after a computer has failed or been replaced, for instance.

You should always store the operating parameter settings, the partner list and, where applicable, the FTAC environment in backup files. To do this, you can proceed as follows (the filenames are only examples and the backup files must not already exist):

- Backing up the operating parameter settings:

  ```
  /ASSIGN-SYSLST TO=OPTION-FILE
  ```

  ```
  /SH-FT-OPT OUTPUT=*SYSLST(*BS2-PROC)
  ```

  ```
  /ASSIGN-SYSLST TO=*PRIMARY
  ```

  The first column of the file created (in the example, this is OPTION-FILE) contains print control characters. This means that you must subsequently delete the first column.

- Backing up partner list entries:

  ```
  /START-OPENFTPART PARTBS2.SAV
  ```

- Backing up the FTAC environment:

  ```
  /EXPORT-FTAC-ENV FTACBS2.SAV
  ```

4 Central administration

Central administration in openFT covers the functions **remote administration** and **ADM traps**. openFT for BS2000/OSD supports both functions and can thus be integrated in an overall strategy.

These functions offer considerable advantages that are of particular benefit if you want to administer and monitor a large number of openFT instances, e.g.:

- Simple configuration

  The configuration data is maintained centrally on the **remote administration server**, which means that it only exists once. The creation of roles in the form of **remote administrators** and the grouping of several instances make it possible to implement even complex configurations simply and in a clearly structured way. Subsequent changes are simple to incorporate and thus make the configuration easy to maintain.

  The remote administration server runs on either a Unix or a Windows system.

- Simplified authentication procedure

  If you wish to use authentication for reasons of security, it is only necessary to distribute a few keys:

  - For the direction to the remote administration server, the keys of computers from which remote administration is to be performed must be stored on the remote administration server.
  - For the direction from the remote administration server to the instances to be administered, it is only necessary to store the public key of the remote administration server on the openFT instances to be administered.

- High performance

  The new remote administration interface allows far longer command sequences than in openFT up to V10.0.

  It is possible to configure the remote administration server in such a way that it is available exclusively for remote administration. In this case, there is no dependency on normal FT operation and hence no mutual impact.

- Simple administration

  Remote administrators only need one (central) transfer admission. Up to openFT V10, the remote administrators had to remember the access data for each openFT instance to be administered.

- Central logging of important events

  ADM traps can be generated if certain events occur on openFT instances. These are sent to the (central) ADM trap server and stored permanently there. This allows remote administrators to evaluate important events at a later time and for specific instances.

- Compatible integration of earlier openFT versions

  Instances running versions of openFT as of V8.0 can simply be added to the configuration and administered in the same way as instances as of V11.0. All the administration functions offered by the corresponding openFT version can be used.

4.1 Remote administration

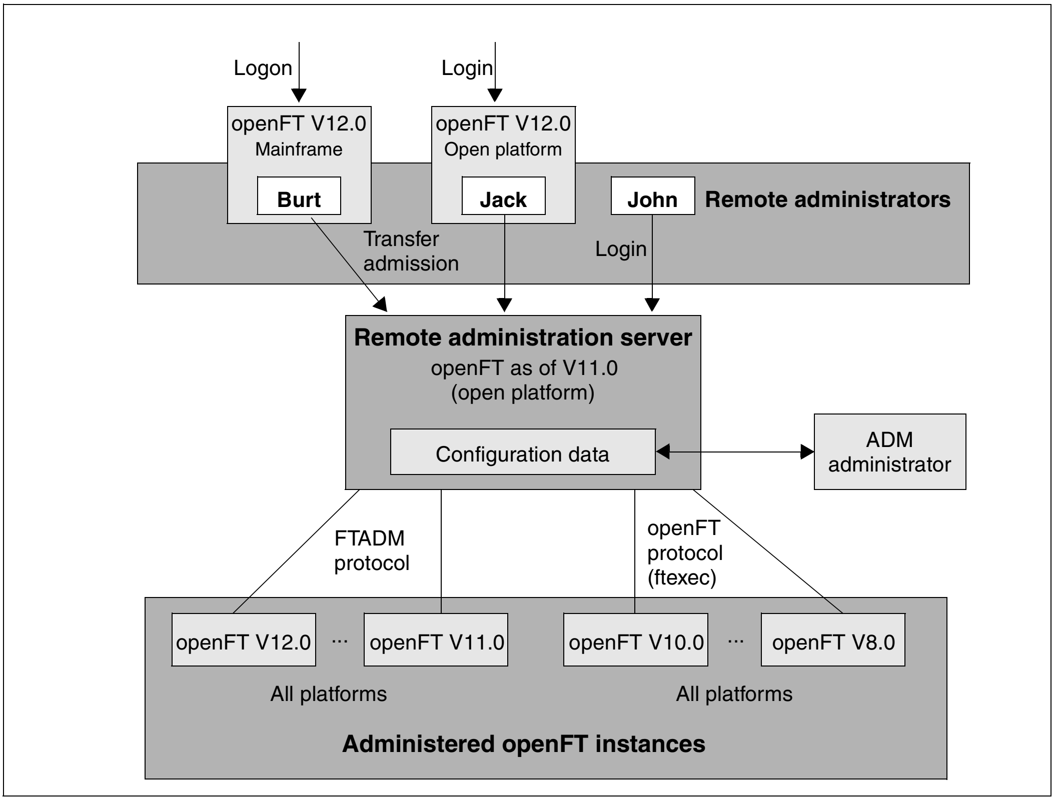
openFT allows you to set up a remote administration server via which you can administer your openFT instances on the various platforms. You can choose to use any openFT instance as an administration workstation.

This section describes:

- the remote administration concept
- how to configure an openFT instance on BS2000/OSD for remote administration
- how to enter remote administration commands on BS2000/OSD

4.1.1 The remote administration concept

The figure below shows the remote administration components and the most important configuration options on the basis of a deployment scenario.



Remote administration components

Remote administration comprises the following components:

Remote administration server

Central remote administration component. This runs on a Unix or Windows system with openFT as of V11.0 and contains all configuration data for remote administration.

Multiple remote administration servers can be defined in a complete configuration.

i You will find details on configuring a remote administration server in the openFT manuals "openFT V12.0 for Unix Systems - Installation and Administration" and "openFT V12.0 for Windows Systems - Installation and Administration".

ADM administrator

Person who administers the remote administration server. This person creates the configuration data for remote administration in which, for instance, the remote administrators and the administered openFT instances are defined. The ADM administrator is the only person permitted to change the configuration data.

Remote administrator

Role configured on the remote administration server and which grants permission to execute certain administration functions on certain openFT instances. A remote administrator can

- Log in directly at the remote administration server (single sign-on)
- Log in to a different openFT instance (as of V11.0) and access the remote administration server using an FTAC transfer admission.
  The openFT instance can be running either on a mainframe (BS2000/OSD, z/OS) or on a Unix or Windows system. The FTADM protocol is used for communication.

Several remote administrators can be configured with different permissions.

Administered openFT instance

openFT instance that is able to be administered by remote administrators during live operation. Access is via an admission profile. The following applies, depending on the openFT version of the openFT instance:

- In the case of openFT instances as of V11.0, the FTADM protocol is used, and the full range of remote administration functions can be utilized.
- In the case of openFT instances from V8.0 through V10.0, administration is carried out using the openFT protocol and the command *ftexec*. The range of functions available depends on the openFT version of the instance being administered.

4.1.2 Configuring an openFT instance on BS2000/OSD for remote administration

The remote administration server uses FTAC transfer admissions to access the openFT instances. This means that the appropriate admission profiles must be defined in the openFT instances from which administration is being carried out.

To enable a remote administrator to access the openFT instance, the FT administrator sets up an admission profile on the BS2000/OSD system using the REMOTE-ADMINISTRATION function:

```
/CREATE-FT-PROFILE NAME=profile                             -
/         ,TRANSFER-ADMISSION=transfer admission      -
/         ,PARTNER=remote administration server       -
/         ,FT-FUNCTION=*REMOTE-ADMINISTRATION
```

The ADM administrator specifies the FTAC transfer admission in the configuration file of the remote administration server when defining the openFT instance. For an example, see the manual "openFT V12.0 for Unix Systems - Installation and Administration". The operand PARTNER= ensures that this profile can only be used by the remote administration server.

Entering the remote administration server in the partner list

If remote administration requests are to be issued from your BS2000 system, the FT administrator can enter the remote administration server in the partner list. This has the advantage that you can explicitly assign particular attributes to this partner, for instance the security level or the trace settings.

The FT administrator enters the remote administration server in the partner list using the following format:

```
ftadm://host[:port number]
```

You only specify *port number* if the default ADM port (11000) is not used on the remote administration server *host*. The same applies if a remote administrator specifies the address directly in a remote administration request.

4.1.3 Issuing remote administration requests

If you wish to enter remote administration requests, you require the following:

- the name of the remote administration server in the partner list or the address of the remote administration server (ask the FT administrator if necessary)
- the transfer admission for accessing the remote administration server. The ADM administrator of the remote administration server must make this available to you.

You are able to determine the names of the openFT instances that you are permitted to administer yourself.

Determining the names of the openFT instances

The ADM administrator defines the names of the openFT instances during configuration of the remote administration server. You get the names of the openFT instances by executing the ftshwc command as a remote administration command on the remote administration server:

```
/EXECUTE-REMOTE-FTADM-CMD PARTNER-SERVER=server  -
/         ,TRANSFER-ADMISSION=transfer admission -
/        ,ROUTING-INFO=*NONE                     -
/        ,CMD='ftshwc -rt=i'
```

Explanation

server
: Name of the remote administration server from the partner list. Alternatively, you can also enter the address directly in the format *ftadm://host...*

transfer admission
: FTAC transfer admission on the remote administration server.

'ftshwc -rt=i'
: 'ftshwc -rt=i' is a command executed on the remote administration server that outputs the names of the instances that you are permitted to administer. You must enter the quotes.

Sample output

```
TYPE    = *INSTANCE     ACCESS = FT+FTOP          MODE = FTADM
   NAME = Muenchen/MCH1/OPENFT01
   DESC = Windows Server 2008
TYPE    = *INSTANCE     ACCESS = FT+FTOP          MODE = FTADM
   NAME = Muenchen/MCH1/OPENFT02
   DESC = Solaris
TYPE    = *INSTANCE     ACCESS = FTOP             MODE = LEGACY
   NAME = Muenchen/MCH1/OPENFT03
   DESC = Windows Server 2003
TYPE    = *INSTANCE     ACCESS = FT+FTOP+FTAC     MODE = FTADM
   NAME = Muenchen/MCH2/MCHSRV03
```

NAME specifies the name of the instance that you must specify exactly as given here in the remote administration request. Your remote administration permissions for this instance are listed under ACCESS. See also Abschnitt „Remote administration commands“ auf Seite 193. MODE specifies whether the instance is administered via the FTADM protocol (MODE=FTADM) or via ftexec (MODE=LEGACY).

Issuing a remote administration request

Specify the remote administration command in the following form:

```
/EXECUTE-REMOTE-FTADM-CMD PARTNER-SERVER=server   -
/         ,TRANSFER-ADMISSION=transfer admission  -
/        ,ROUTING-INFO=instance                   -
/        ,CMD='command'
```

Explanation

server

Name of the remote administration server from the partner list. Alternatively, you can also enter the address directly in the format *ftadm://host...*

transfer admission

FTAC transfer admission on the remote administration server.

instance

Routing name of the openFT instance on which the administration command is to be executed. You must enter this name in exactly the form in which it appears on the remote administration server with the ftshwc command. See „Determining the names of the openFT instances“ auf Seite 104.

command

Specifies the administration command to be executed on the openFT instance. For further details, see Abschnitt „EXECUTE-REMOTE-FTADM-CMD Execute remote administration command“ auf Seite 190.

4.1.4 Logging remote administration

ADM log records are created in each of the openFT instances involved when remote administration requests are issued.

ADM log records are explicitly flagged as being of a particular type (A). They are handled in a similar way to FT or FTAC log records, i.e. you can view ADM log records in BS2000/OSD using the SHOW-FT-LOGGING-RECORDS command (see Seite 315) and delete them with the DELETE-FT-LOGGING-RECORDS command (provided that you have the appropriate permission to do so, see Seite 182).

Controlling ADM logging

The FT administrator controls the scope of ADM logging using the operating parameters. The following options are available:

- log all administration requests
- log all administration requests that modify data
- log administration requests during which errors occurred
- disable ADM logging

You do this by means of the MODIFY-FT-OPTIONS command with the operand LOGGING= *SELECT(ADM=...)

4.2 ADM traps

ADM traps are short messages that openFT sends to the **ADM trap server** if certain events occur during operation of openFT. Such events may include errored FT requests, status changes or the unavailability of partners, for instance.

The ADM traps are stored permanently on the ADM trap server. This allows one or more openFT systems to be monitored at a central location. The FT administrator of the ADM trap server is thus provided with a simple way of gaining an overview of events that have occurred on the openFT instances he is monitoring.

If the ADM trap server is simultaneously used as a remote administration server, remote administrators can also view traps from other systems and hence monitor the systems that they are administering. This means that if you are a remote administrator, you can view the ADM traps of "your" administered instances on the BS2000.

4.2.1 Configuring ADM traps in the openFT instance

To allow ADM traps from your openFT instance on the BS2000/OSD system to be sent to the ATM trap server, you must carry out the following actions in your role as FT administrator:

- Enter the address and admission data for the ADM trap server
- Specify the scope of the ADM traps sent to the ADM trap server

In addition, the FT administrator of the ADM trap server must set up a corresponding admission profile on the ADM trap server.

Enter the address and admission data for the ADM trap server

You specify the address and the transfer admission of the ADM trap server in the ADM-TRAPS operand of the MODIFY-FT-OPTIONS command:

```
/MODIFY-FT-OPTIONS ...                                             -
/         ,ADM-TRAPS=*PAR(DESTINATION=(PARTNER=adm-trap-server,    -
/                      TRANSFER-ADMISSION=trap-admission))
```

adm-trap-server

must be defined in the partner list using the address format *ftadm://host...*. Alternatively, you can also enter the address directly in the format *ftadm://host...*

trap-admission

is the transfer admission for the admission profile defined in the ADM trap server for this purpose.

Specify the scope of the ADM traps

The scope of the ADM traps sent to the ADM trap server is controlled using the operating parameters. You can set which of the events listed below cause traps to be sent:

- Change of openFT status (START-FT / STOP-FT)
- Change of partner status
- Unavailability of partners
- Change of request management status
- Successfully completed requests
- Failed requests

To do this, use the MODIFY-FT-OPTIONS command and defying the required selection under SELECTION in the ADM-TRAPS operand.

4.2.2 Viewing ADM traps

The FT administrator of the ADM trap server is permitted to view all ADM traps on the ADM trap server. If the ADM trap server is also used as the remote administration server, the remote administrators can also view traps.

If you log on to your BS2000 system as a remote administrator, you can view your "own" ADM traps. These are the ADM traps of those openFT instances for which you have at least FTOP permission. See the „Determining the names of the openFT instances“ auf Seite 104.

If you wish to view the most recent 10 ADM traps, enter the following remote administration command:

```
/EXECUTE-REMOTE-FTADM-CMD PARTNER-SERVER=server  -
/         ,TRANSFER-ADMISSION=transfer admission -
/        ,ROUTING-INFO=*NONE                     -
/        ,CMD='ftshwatp -nb=10'
```

Explanation

server
: Name of the remote administration server from the partner list. Alternatively, you can also enter the address directly in the format *ftadm://host...*

transfer admission
: FTAC transfer admission on the remote administration server.

'ftshwatp -nb=10'
: 'ftshwatp -nb=10' is a command executed on the remote administration server that outputs the last 10 ADM traps. You must enter the quotes.

The ftshwatp command also provides further options. For details, see, for instance, the manual "openFT V12.0 for Unix Systems - Installation and Administration".

5 Command interface

openFT for BS2000 offers a new SDF command interface for administration.
The FT administration commands can be issued from the console. Administration from the terminal requires the FT-ADMINISTRATION privilege, which is assigned by default to the TSOS ID. If SECOS is in use, this privilege can also be assigned to other user IDs. See the SECOS manual for details.
The FT administrator commands that may be entered via the console, can also be set by all the IDs with the OPERATING privilege. If necessary, this privilege can be taken away from these IDs.
These are the commands: ADD-FT-PARTNER, CREATE-FT-INSTANCE, CREATE-FT-KEY-SET, DELETE-FT-INSTANCE, DELETE-FT-KEY-SET, MODIFY-FT-INSTANCE, MODIFY-FT-OPTIONS, MODIFY-FT-PARTNER, REMOVE-FT-PARTNER, SHOW-FT-OPTIONS, SHOW-FT-PARTNER, START-FT, STOP-FT, UPDATE-FT-PUBLIC-KEYS.

5.1 Functional command overview

The following overview shows the FT and FTAC administrator commands as they relate to individual jobs. The following user groups are distinguished here:

FT user
Person who uses functions of the product openFT but has no rights as FT administrator.

FT administrator
Person who manages the product openFT on a computer.

FTAC user
Person who can manage admission records for his/her own user ID but does not have the rights of an FTAC administrator.

FTAC administrator
Person who manages the product openFT-AC on a computer.

5.1.1 FT command overview

Administer openFT partners

Add partner to the partner list	ADD-FT-PARTNER	page 136
Remove partner from the partner list	REMOVE-FT-PARTNER	page 282
Modify partner properties	MODIFY-FT-PARTNER	page 249
Display partner systems	SHOW-FT-PARTNERS	page 363
List partner systems as command procedure	START-OPENFTPART	page 385

Activate and deactivate openFT

Activate openFT	START-FT	page 383
Deactivate openFT	STOP-FT	page 386

Controlling openFT operating parameters

Modify operating parameters	MODIFY-FT-OPTIONS	page 223
Display operating parameters	SHOW-FT-OPTIONS	page 351

Administer key pair sets for authentication

Create a key pair set	CREATE-FT-KEY-SET	page 155
Import keys	IMPORT-FT-KEY	page 204
Display key properties	SHOW-FT-KEY	page 311
Update public keys	UPDATE-FT-PUBLIC-KEYS	page 388
Modify keys	MODIFY-FT-KEY	page 221
Delete a key pair set	DELETE-FT-KEY-SET	page 180

Administering openFT instances

Create openFT instance	CREATE-FT-INSTANCE	page 153
Delete openFT instance	DELETE-FT-INSTANCE	page 179
Modify openFT instance	MODIFY-FT-INSTANCE	page 219

Remote administration

Issue remote administration command	EXECUTE-REMOTE-FTADM-CMD	page 190

Manage request queue

Cancel FT requests	CANCEL-FILE-TRANSFER	page 147
Show information on FT requests	SHOW-FILE-TRANSFER	page 284
Modify FT request queue	MODIFY-FILE-TRANSFER	page 207

Logging Function

Delete log records or offline log files	DELETE-FT-LOGGING-RECORDS	page 182
Show log records or log files	SHOW-FT-LOGGING-RECORDS	page 315

Monitoring

Show monitoring data	SHOW-FT-MONITOR-VALUES	page 337

A destailed description of the FT command START-FTTRACE for evaluating traces is provided in the section “START-FTTRACE” on page 94.

5.1.2 FTAC commands overview

openFT-AC must be installed in order to use the following commands:

Edit FTAC admission profiles

Create admission profile	CREATE-FT-PROFILE	page 157
Delete admission profile	DELETE-FT-PROFILE	page 187
Modify admission profile	MODIFY-FT-PROFILE	page 257
Show admission profile	SHOW-FT-PROFILE	page 372

Edit FTAC admission sets

Modify admission set	MODIFY-FT-ADMISSION-SET	page 213
Show admission set	SHOW-FT-ADMISSION-SET	page 306

Store and display saved FTAC admission profiles and sets

Export admission profiles and sets	EXPORT-FTAC-ENVIRONMENT	page 199
Import admission profiles and sets	IMPORT-FTAC-ENVIRONMENT	page 201
Display saved admission profiles and sets	SHOW-FTAC-ENVIRONMENT	page 302

Show partner systems

Display partner systems and security levels	SHOW-FT-RANGE	page 380

5.2 Entering FT commands

Please remember the following when entering commands:

- You must insert commas to separate the individual operands of a command, e.g.

  ```
  /TRANSFER-FILE TRANSFER-DIRECTION=TO,PARTNER=ZENTRALE,LOCAL-PARAMETER=...
  ```

- If quotes appear in a value assignment which is itself enclosed in quotes, they must be entered twice.
- If there is no default value marked (by underscoring) for an operand, then it **must** be specified with a valid value (mandatory operand).
- A distinction is made between positional operands and keyword operands. Positional operands are uniquely determined by their position in the command. Keyword operands are uniquely determined by their keyword, for example `TRANSFER-DIRECTION=...` There are a number of considerations to be borne in mind when specifying such operands (see below).
- You can abbreviate your entries for commands and operands, always ensuring that your entries retain their uniqueness. You can also use positional operands if you wish. Short forms and long forms can be mixed at will. Certain abbreviated forms of keywords and a number of positional operands are guaranteed for openFT. In the command representation the recommended abbreviation is shown in **bold**. This means that you will find these options unchanged in subsequent versions. This means, therefore, that to be “on the safe side”, you should form the habit of entering these commands in their abbreviated form. You should take particular care to use the guaranteed abbreviated forms in procedures, as this will ensure their continued executability in subsequent versions. The recommended abbreviations are used in the examples shown in this chapter. The possible abbreviations are listed for the individual command formats.
- If a structure is preceded by an introductory operand value, then the opening parentheses must immediately follow this operand value. Example: *BS2000 is an introductory operand value in REM=*BS2000(...). Introductory operand values may be omitted if there is no risk of ambiguity.
- The asterisk (*) that precedes constant operand values may be omitted if there is no risk of ambiguity. Please ensure that it is not a guaranteed abbreviation.

When you enter commands, the value assignments for the operands may be specified in positional form, in keyword form or in mixed form.
Please note the following:

- When you perform value assignments in positional form, the first value is assigned to the first operand in the command, the second value to the second operand etc.
- Values assigned in positional form are separated by commas. You must also enter a comma for each operand for which no value is assigned.
- If two values are assigned to an operand, the last value to be assigned always applies. This also applies to parameter specifications in introductory operand values within the corresponding structure brackets. However, for the sake of clarity, double assignments should generally be avoided.
- If you mix the different forms of operand value assignments (positional and keyword form), then you must observe the correct sequence. Note that you can start your input with positional operands and follow these with keyword operands but not the other way round!
- Since there is a possibility that the sequence of operands may change in subsequent versions, only keyword operands should be used in procedures.

5.3 Command syntax representation

The following example shows the representation of the syntax of a command in a manual. The command format consists of a field with the command name. All operands with their legal values are then listed. Operand values which introduce structures and the operands dependent on these operands are listed separately.

```
HELP-SDF                                                     Alias: HPSDF

 GUIDANCE-MODE = *NO / *YES
,SDF-COMMANDS = *NO / *YES
,ABBREVIATION-RULES = *NO / *YES
,GUIDED-DIALOG = *YES(...)
    *YES(...)
      |  SCREEN-STEPS = *NO / *YES
      | ,SPECIAL-FUNCTIONS = *NO / *YES
      | ,FUNCTION-KEYS = *NO / *YES
      | ,NEXT-FIELD = *NO / *YES
,UNGUIDED-DIALOG = *YES(...) / *NO
    *YES(...)
      |  SPECIAL-FUNCTIONS = *NO / *YES
      | ,FUNCTION-KEYS = *NO / *YES
```

Representation of the syntax of the user command HELP-SDF

This syntax description is valid for SDF V4.6A.The syntax of the SDF command/statement language is explained in the following three tables.

table 1: Notational conventions

The meanings of the special characters and the notation used to describe command and statement formats are explained in table 1.

table 2: Data types

Variable operand values are represented in SDF by data types. Each data type represents a specific set of values. The number of data types is limited to those described in table 2.

The description of the data types is valid for the entire set of commands/statements. Therefore only deviations (if any) from the attributes described here are explained in the relevant operand descriptions.

table 3: Suffixes for data types

Data type suffixes define additional rules for data type input. They contain a length or interval specification. They can be used to limit the set of values (suffix begins with *without*), extend it (suffix begins with *with*), or declare a particular task mandatory (suffix begins with *mandatory*). The following short forms are used in this manual for data type suffixes:

cat-id	cat
completion	compl
correction-state	corr
generation	gen
lower-case	low
manual-release	man
odd-possible	odd
path-completion	path-compl
separators	sep
temporary-file	temp-file
under-score	under
user-id	user
version	vers
wildcard-constr	wild-constr
wildcards	wild

The description of the 'integer' data type in Table 3 contains a number of items in italics which are not part of the syntax. They are only used to make the table easier to read. For special data types that are checked by the implementation, Table 3 contains suffixes printed in italics (see the *special* suffix) which are not part of the syntax.

The description of the data type suffixes is valid for the entire set of commands/statements. Therefore only deviations (if any) from the attributes described here are explained in the relevant operand descriptions.

Metasyntax

Representation	Meaning	Examples
UPPERCASE LETTERS	Uppercase letters denote keywords (command, statement or operand names, keyword values) and constant operand values. Keyword values begin with *	HELP-SDF SCREEN-STEPS = *NO
UPPERCASE LETTERS in boldface	Uppercase letters printed in boldface denote guaranteed or suggested abbreviations of keywords.	GUIDANCE-MODE = *YES
=	The equals sign connects an operand name with the associated operand values.	GUIDANCE-MODE = *NO
< >	Angle brackets denote variables whose range of values is described by data types and suffixes (see Tables 2 and 3)).	SYNTAX-FILE = <filename 1..54>
Underscoring	Underscoring denotes the default value of an operand.	GUIDANCE-MODE = *NO
/	A slash serves to separate alternative operand values.	NEXT-FIELD = *NO / *YES
(…)	Parentheses denote operand values that initiate a structure.	,UNGUIDED-DIALOG = *YES(...) / *NO
[ ]	Square brackets denote operand values which introduce a structure and are optional. The subsequent structure can be specified without the initiating operand value.	SELECT = [*BY-ATTRIBUTES](...)
Indentation	Indentation indicates that the operand is dependent on a higher-ranking operand.	,GUIDED-DIALOG = *YES(...) *YES(...) │ SCREEN-STEPS = *NO / │ *YES

Table 1: Metasyntax (part 1 of 2)

Representation	Meaning	Examples
|	A vertical bar identifies related operands within a structure. Its length marks the beginning and end of a structure. A structure may contain further structures. The number of vertical bars preceding an operand corresponds to the depth of the structure.	**SUP**PORT = ***TAPE**(...) ***TAPE(...)** | **VOL**UME = ***ANY**(...) | ***ANY**(...) | | ...
,	A comma precedes further operands at the same structure level.	**GUID**ANCE-**MODE** = ***NO** / ***Y**ES ,**SDF-COM**MANDS = ***NO** / ***Y**ES
list-poss(n):	The entry “list-poss” signifies that a list of operand values can be given at this point. If (n) is present, it means that the list must not have more than n elements. A list of more than one element must be enclosed in parentheses.	list-poss: ***SAM** / ***ISAM** list-poss(40): <structured-name 1..30> list-poss(256): ***OMF** / ***SYSLST**(...) / <filename 1..54>
Alias:	The name that follows represents a guaranteed alias (abbreviation) for the command or statement name.	**HELP-SDF** Alias: **HPSDF**

Table 1: Metasyntax (part 2 of 2)

Data types

Data type	Character set	Special rules
alphanum-name	A…Z 0…9 $, #, @	
cat-id	A…Z 0…9	Not more than 4 characters; must not begin with the string PUB
command-rest	freely selectable	
composed-name	A…Z 0…9 $, #, @ hyphen period catalog ID	Alphanumeric string that can be split into multiple substrings by means of a period or hyphen. If a file name can also be specified, the string may begin with a catalog ID in the form :cat: (see data type filename).
c-string	EBCDIC character	Must be enclosed within single quotes; the letter C may be prefixed; any single quotes occurring within the string must be entered twice.
date	0…9 Structure identifier: hyphen	Input format: yyyy-mm-dd yyyy: year; optionally 2 or 4 digits mm: month dd: day Only date specifications between 1.1.2000 and 19.1.2038 are possible. If the year is specified in 2-digit form, 2000 is added to the number
device	A…Z 0…9 hyphen	Character string, max. 8 characters in length, corresponding to a device available in the system. In guided dialog, SDF displays the valid operand values. For notes on possible devices, see the relevant operand description.

Table 2: Data types (part 1 of 6)

Data type	Character set	Special rules
fixed	+, - 0…9 period	Input format: [sign][digits].[digits] [sign]: + or - [digits]: 0...9 must contain at least one digit, but may contain up to 10 characters (0...9, period) apart from the sign.
filename	A…Z 0…9 $, #, @ hyphen period	Input format: $[\text{:cat:}][\text{\$user.}]\left\{\begin{array}{l}\text{file}\\ \text{file(no)}\\ \text{group}\\ \text{group}\left\{\begin{array}{l}\text{(*abs)}\\ \text{(+rel)}\\ \text{(-rel)}\end{array}\right\}\end{array}\right\}$:cat: optional entry of the catalog identifier; character set restricted to A...Z and 0...9; maximum of 4 characters; must be enclosed in colons; default value is the catalog identifier assigned to the user ID, as specified in the user catalog. $user. optional entry of the user ID; character set is A…Z, 0…9, $, #, @; maximum of 8 characters; first character cannot be a digit; $ and period are mandatory; default value is the user's own ID. $. (special case) system default ID

Table 2: Data types (part 2 of 6)

Data type	Character set	Special rules

filename (cont.)		file
		file or job variable name;
		may be split into a number of partial names using a period as a delimiter:
		name$_1$[.name$_2$[...]]
		name$_i$ does not contain a period and must not begin or end with a hyphen;
		file can have a maximum length of 41 characters; it must not begin with a $ and must include at least one character from the range A...Z.
		#file (special case)
		@file (special case)
		# or @ used as the first character indicates temporary files or job variables, depending on system generation.
		file(no)
		tape file name
		no: version number;
		character set is A...Z, 0...9, $, #, @.
		Parentheses must be specified.
		group
		name of a file generation group
		(character set: as for “file”)
		group$\left\{\begin{array}{l}(\text{*abs})\\(\text{+rel})\\(\text{-rel})\end{array}\right\}$
		(*abs)
		absolute generation number (1-9999);
		* and parentheses must be specified.
		(+rel)
		(-rel)
		relative generation number (0-99);
		sign and parentheses must be specified.

integer	0…9, +, -	+ or -, if specified, must be the first character.
name	A…Z 0…9 $, #, @	Must not begin with 0...9.

Table 2: Data types (part 3 of 6)

Data type	**Character set**	**Special rules**
partial-filename	A…Z 0…9 $, #, @ hyphen period	Input format: [:cat:][$user.][partname.] :cat: see filename $user. see filename partname optional entry of the initial part of a name common to a number of files or file generation groups in the form: $name_1$.[$name_2$.[...]] $name_i$ (see filename). The final character of “partname” must be a period. At least one of the parts :cat:, $user. or partname must be specified.
posix-filename	A...Z 0...9 special characters	String which may have a maximum length of 255 characters. Consists of either one or two periods or of alphanumeric characters and special characters.The special characters must be escaped with a preceding \ (backslash). The / is not allowed. Must be enclosed within single quotes if alternative data types are permitted, separators are used, or the first character is a ?, ! or ^. A distinction is made between uppercase and lowercase.

posix-pathname	A...Z
	0...9
	special characters
	structure identifier: slash
		Input format: [/]$part_1$/.../$part_n$
		where $part_i$ is a posix-filename;
		maximum of 510 in *POSIX syntax;
		must be enclosed within single quotes if alternative data types are permitted, separators are used, or the first character is a ?, ! or ^

Table 2: Data types (part 4 of 6)

Data type	Character set	Special rules
product-version	A…Z 0…9 period single quote	Input format: [[C]'][V][m]m.naso['] correction status release status where m, n, s and o are all digits and a is a letter. Whether the release and/or correction status may/must be specified depends on the suffixes to the data type (see the suffixes without-corr, without-man, mandatory-man and mandatory-corr in table 3). product-version may be enclosed within single quotes (possibly with a preceding C). The specification of the version may begin with the letter V.
structured-name	A…Z 0…9 $, #, @ hyphen	Alphanumeric string which may comprise a number of substrings separated by a hyphen. First character: A...Z or $, #, @
text	freely selectable	For the input format, see the relevant operand descriptions.
time	0…9 structure identifier: colon	Time-of-day entry: Input format: { hh:mm:ss hh:mm hh } hh: hours mm: minutes ss: seconds } Leading zeros may be omitted
vsn	a) A…Z 0…9	a) Input format: pvsid.sequence-no max. 6 characters pvsid: 2-4 characters; PUB must not be entered sequence-no: 1-3 characters
	b) A…Z 0…9 $, #, @	b) Max. 6 characters; PUB may be prefixed, but must not be followed by $, #, @.

Table 2: Data types (part 5 of 6)

Data type	**Character set**	**Special rules**
x-string	Hexadecimal: 00…FF	Must be enclosed in single quotes; must be prefixed by the letter X. There may be an odd number of characters.
x-text	Hexadecimal: 00…FF	Must not be enclosed in single quotes; the letter X must not be prefixed. There may be an odd number of characters.

Table 2: Data types (part 6 of 6)

Suffixes for data types

Suffix	Meaning
x..y *unit*	With data type “integer”: interval specification x minimum value permitted for “integer”. x is an (optionally signed) integer. y maximum value permitted for “integer”. y is an (optionally signed) integer. *unit* with “integer” only: additional units. The following units may be specified: *days* *byte* *hours* *2Kbyte* *minutes* *4Kbyte* *seconds* *Mbyte* milliseconds
x..y *special*	With the other data types: length specification For data types catid, date, device, product-version, time and vsn the length specification is not displayed. x minimum length for the operand value; x is an integer. y maximum length for the operand value; y is an integer. x=y the length of the operand value must be precisely x. *special* Specification of a suffix for describing a special data type that is checked by the implementation. “*special*” can be preceded by other suffixes. The following specifications are used: *arithm-expr* arithmetic expression (SDF-P) *bool-expr* logical expression (SDF-P) *string-expr* string expression (SDF-P) *expr* freely selectable expression (SDF-P) *cond-expr* conditional expression (JV) *symbol* CSECT or entry name (BLS)
with	Extends the specification options for a data type.
-compl	When specifying the data type “date”, SDF expands two-digit year specifications in the form yy-mm-dd to: 20yy-mm-dd if yy < 60 19yy-mm-dd if yy ≥ 60
-low	Uppercase and lowercase letters are differentiated.
-path-compl	For specifications for the data type “filename”, SDF adds the catalog and/or user ID if these have not been specified.

Table 3: Data type suffixes (part 1 of 7)

<table>
<tr><th>Suffix</th><th>Meaning</th></tr>
<tr><td>with (cont.)</td><td></td></tr>
<tr><td>-under</td><td>Permits underscores (_) for the data types “name” and “composed-name”.</td></tr>
<tr><td>-wild(n)</td><td>Parts of names may be replaced by the following wildcards.
n denotes the maximum input length when using wildcards.
Due to the introduction of the data types posix-filename and posix-pathname, SDF now accepts wildcards from the Unix world (referred to below as POSIX wildcards) in addition to the usual BS2000 wildcards. However, as not all commands support POSIX wildcards, their use for data types other than posix-filename and posix-pathname can lead to semantic errors.
Only POSIX wildcards or only BS2000 wildcards should be used within a search pattern. Only POSIX wildcards are allowed for the data types posix-filename and posix-pathname. If a pattern can be matched more than once in a string, the first match is used.
<table>
<tr><th>BS2000 wildcards</th><th>Meaning</th></tr>
<tr><td>*</td><td>Replaces an arbitrary (even empty) character string. If the string concerned starts with *, then the * must be entered twice in succession if it is followed by other characters and if the character string entered does not contain at least one other wildcard.</td></tr>
<tr><td>Terminating period</td><td>Partially-qualified entry of a name.
Corresponds implicitly to the string “./*”, i.e. at least one other character follows the period.</td></tr>
<tr><td>/</td><td>Replaces any single character.</td></tr>
<tr><td>&lt;s_x:s_y&gt;</td><td>Replaces a string that meets the following conditions:
– It is at least as long as the shortest string (s_x or s_y)
– It is not longer than the longest string (s_x or s_y)
– It lies between s_x and s_y in the alphabetic collating sequence; numbers are sorted after letters (A...Z0...9)
– s_x can also be an empty string (which is in the first position in the alphabetic collating sequence)
– s_y can also be an empty string, which in this position stands for the string with the highest possible code (contains only the characters X'FF')</td></tr>
</table>
</td></tr>
</table>

Table 3: Data type suffixes (part 2 of 7)

Suffix	**Meaning**	
	<s_1,…>	Replaces all strings that match any of the character combinations specified by s. s may also be an empty string. Any such string may also be a range specification “s_x:s_y” (see above).
with-wild(n)		
	-s	Replaces all strings that do not match the specified string s. The minus sign may only appear at the beginning of string s. Within the data types filename or partial-filename the negated string -s can be used exactly once, i.e. -s can replace one of the three name components: cat, user or file.
	Wildcards are not permitted in generation and version specifications for file names. Only system administration may use wildcards in user IDs. Wildcards cannot be used to replace the delimiters in name components cat (colon) and user ($ and period).	
	POSIX wildcards	Meaning
	*	Replaces any single string (including an empty string). An * appearing at the first position must be duplicated if it is followed by other characters and if the entered string does not include at least one further wildcard.
	?	Replaces any single character. It is not permitted as the first character outside single quotes.
	[c_x-c_y]	Replaces any single character from the range defined by c_x and c_y, including the limits of the range. c_x and c_y must be normal characters.
	[s]	Replaces exactly one character from string s. The expressions [c_x-c_y] and [s] can be combined into [$s_1$$c_x$-$c_y$$s_2$].
	[!c_x-c_y]	Replaces exactly one character not in the range defined by c_x and c_y, including the limits of the range. c_x and c_y must be normal characters. The expressions [!c_x-c_y] and [!s] can be combined into [!$s_1$$c_x$-$c_y$$s_2$].
	[!s]	Replaces exactly one character not contained in string s. The expressions [!s] and [!c_x-c_y] can be combined into [!$s_1$$c_x$-$c_y$$s_2$].

Table 3: Data type suffixes (part 3 of 7)

<table>
<tr><th>Suffix</th><th colspan="2">Meaning</th></tr>
<tr><td>with (cont.)</td><td colspan="2"></td></tr>
<tr><td rowspan="7">-wild-constr(n)</td><td colspan="2">Specification of a constructor (string) that defines how new names are to be constructed from a previously specified selector, i.e., a selection string with wildcards (see also with-wild). n denotes the maximum input length when using wildcards.
The constructor may consist of constant strings and patterns. A pattern (character) is replaced by the string that was selected by the corresponding pattern in the selector.
The following wildcards may be used in constructors:</td></tr>
<tr><td>Wildcard</td><td>Meaning</td></tr>
<tr><td>*</td><td>Corresponds to the string selected by the wildcard * in the selector.</td></tr>
<tr><td>Terminating period</td><td>Corresponds to the partially-qualified specification of a name in the selector.
Corresponds to the string selected by the terminating period in the selector.</td></tr>
<tr><td>/ or ?</td><td>Corresponds to the character selected by the / or ? wildcard in the selector.</td></tr>
<tr><td><n></td><td>Corresponds to the string selected by the n-th wildcard in the selector, where n is an integer.</td></tr>
<tr><td colspan="2">Allocation of wildcards to corresponding wildcards in the selector:
All wildcards in the selector are numbered from left to right in ascending order (global index).
Identical wildcards in the selector are additionally numbered from left to right in ascending order (wildcard-specific index).
Wildcards can be specified in the constructor by one of two mutually exclusive methods:
1. Wildcards can be specified via the global index: <n>
2. The same wildcard may be specified as in the selector; substitution occurs on the basis of the wildcard-specific index. For example: the second “/” corresponds to the string selected by the second “/” in the selector</td></tr>
</table>

Table 3: Data type suffixes (part 4 of 7)

Suffix	Meaning
with-wild-constr(n) (continued)	The following rules must be observed when specifying a constructor: – The constructor can only contain wildcards of the selector. – If the string selected by the wildcard <...> or [...] is to be used in the constructor, the index notation must be selected. – The index notation must be selected if the string identified by a wildcard in the selector is to be used more than once in the constructor. For example: if the selector “A/” is specified, the constructor “A<n><n>” must be specified instead of “A//”. – The wildcard * can also be an empty string. Note that if multiple asterisks appear in sequence (even with further wildcards), only the last asterisk can be a non-empty string, e.g. for “****” or “*//*”. – Valid names must be produced by the constructor. This must be taken into account when specifying both the constructor and the selector. – Depending on the constructor, identical names may be constructed from different names selected by the selector. For example: “A/*” selects the names “A1” and “A2”; the constructor “B*” generates the same new name “B” in both cases. To prevent this from occurring, all wildcards of the selector should be used at least once in the constructor. – If the selector ends with a period, the constructor must also end with a period (and vice versa). The string selected by the terminating period in the constructor cannot be specified via the global index.

Table 3: Data type suffixes (part 5 of 7)

<table>
<tr><th>Suffix</th><th>Meaning</th></tr>
<tr><td>with-wild-constr(n) (continued)</td><td>Examples:
<table>
<tr><td>Selector</td><td>Selection</td><td>Constructor</td><td>New name</td></tr>
<tr><td>A//*</td><td>AB1
AB2
A.B.C</td><td>D&lt;3&gt;&lt;2&gt;</td><td>D1
D2
D.CB</td></tr>
<tr><td>C.&lt;A:C>/&lt;D,F&gt;</td><td>C.AAD
C.ABD
C.BAF
C.BBF</td><td>G.&lt;1&gt;.<3>.XY&lt;2&gt;</td><td>G.A.D.XYA
G.A.D.XYB
G.B.F.XYA
G.B.F.XYB</td></tr>
<tr><td>C.&lt;A:C>/&lt;D,F&gt;</td><td>C.AAD
C.ABD
C.BAF
C.BBF</td><td>G.&lt;1&gt;.<2>.XY&lt;2&gt;</td><td>G.A.A.XYA
G.A.B.XYB
G.B.A.XYA
G.B.B.XYB</td></tr>
<tr><td>A//B</td><td>ACDB
ACEB
AC.B
A.CB</td><td>G/XY/</td><td>GCXYD
GCXYE
GCXY. [1]
G.XYC</td></tr>
</table>
[1] The period at the end of the name may violate naming conventions (e.g. for fully-qualified file names).</td></tr>
<tr><td>without</td><td>Restricts the specification options for a data type.</td></tr>
<tr><td>-cat</td><td>Specification of a catalog ID is not permitted.</td></tr>
<tr><td>-corr</td><td>Input format: [[C]'][V][m]m.na[']
Specifications for the data type product-version must not include the correction status.</td></tr>
<tr><td>-gen</td><td>Specification of a file generation or file generation group is not permitted.</td></tr>
<tr><td>-man</td><td>Input format: [[C]'][V][m]m.n[']
Specifications for the data type product-version must not include either release or correction status.</td></tr>
<tr><td>-odd</td><td>The data type x-text permits only an even number of characters.</td></tr>
<tr><td>-sep</td><td>With the data type “text”, specification of the following separators is not permitted: ; = ( ) &lt; &gt; ␣ (i.e. semicolon, equals sign, left and right parentheses, greater than, less than, and blank).</td></tr>
<tr><td>-temp-file</td><td>Specification of a temporary file is not permitted (see #file or @file under filename).</td></tr>
</table>

Table 3: Data type suffixes (part 6 of 7)

Suffix	Meaning
without (cont.)	
-user	Specification of a user ID is not permitted.
-vers	Specification of the version (see “file(no)”) is not permitted for tape files.
-wild	The file types posix-filename and posix-pathname must not contain a pattern (character).
mandatory	Certain specifications are necessary for a data type.
-corr	Input format: [[C]'][V][m]m.naso['] Specifications for the data type product-version must include the correction status and therefore also the release status.
-man	Input format: [[C]'][V][m]m.na[so]['] Specifications for the data type product-version must include the release status. Specification of the correction status is optional if this is not prohibited by the use of the suffix without-corr.
-quotes	Specifications for the data types posix-filename and posix-pathname must be enclosed in single quotes.

Table 3: Data type suffixes (part 7 of 7)

Meaning of operands

After the format of each command there is a detailed description of all the operands, the possible value assignments and their functions.

Otherwise the same metasyntax is used in describing operands as in the representation of the command formats (see above).

5.4 Command return codes

The openFT commands supply return codes that you can query when using SDF-P. Each return code consists of a subcode1 (SC1), a subcode2 (SC2) and the maincode (MC).

Subcode1

Subcode1 represents the error class. It is a decimal number. The possible error classes are:

- No error:
  the value of subcode1 is 0.
- Syntax error:
  the value of subcode1 is between 1 and 31, inclusive.
- Internal error (system error):
  the value of subcode1 is 32.
- Errors not assigned to any other class:
  the value of subcode1 is between 64 and 127, inclusive. If the value of subcode 1 is in this range, the maincode must be evaluated in order to ascertain the appropriate action.
- Command cannot be executed at this time:
  the value of subcode1 is between 128 and 130, inclusive.

Subcode2

Subcode2 either contains information supplementary to that in subcode1 or is equal to 0.

Maincode

The maincode corresponds to the message key of the SYSOUT message. You can use the /HELP-MSG-INFORMATION command to fetch detailed information.

The command return codes are always located after the detailed description of the command. In each case, the corresponding section specifies which command return codes are possible and what their meaning is.

You will find the corresponding specifications in the “Administration commands” section of this manual and in the “User commands” section of the openFT User Guide.

5.5 OPS variables

With OPS (Output Presentation Service), you have the option to create the outputs of SHOW commands alternative or additional to the output in SYSLST/SYSOUT in OPS variables. For this to be possible, SDF-P must be installed. The user must generate the corresponding OPS variables with DECLARE-VARIABLE. The information supplied by SHOW commands is stored by openFT in an SDF-P structure, which can be evaluated with the help of an SDF-P procedure. Structure elements which have not been set due to a corresponding command input are output without value assignment.

The request to set OPS variables is made by integrating the unchanged FT command into the BS2000 command EXEC-CMD.

Example

```
/DECLARE-VARIABLE VARIABLE-NAME=<variable-name>,TYPE=*STRUCTURE(...)...
```

```
/EXEC-CMD (SHOW-FILE-TRANSFER),TEXT=*N,STRUCT-OUT=<variable-name>
```

The following openFT user commands offer OPS support:

- SHOW-FILE-TRANSFER
- SHOW-FILE-FT-ATTRIBUTES
- SHOW-FTAC-ENVIRONMENT
- SHOW-FT-ADMISSION-SET
- SHOW-FT-INSTANCE *
- SHOW-FT-KEY
- SHOW-FT-LOGGING-RECORDS
- SHOW-FT-MONITOR-VALUES
- SHOW-FT-OPTIONS
- SHOW-FT-PARTNERS
- SHOW-FT-PROFILE
- SHOW-FT-RANGE
- SHOW-REMOTE-FILE-ATTRIBUTES *

  * see User Guide

5.6 Output in CSV format

The output of some SHOW commands in openFT and openFT-AC can be optionally requested in CSV (**C**haracter **S**eparated **V**alues) format. CSV is a popular format in the PC environment in which tabular data is defined by lines. Output in CSV format is offered for the following commands:

- SHOW-FILE-TRANSFER
- SHOW-FILE-FT-ATTRIBUTES *
- SHOW-FTAC-ENVIRONMENT
- SHOW-REMOTE-FILE-ATTRIBUTES *
- SHOW-FT-ADMISSION-SET
- SHOW-FT-KEY
- SHOW-FT-LOGGING-RECORDS
- SHOW-FT-MONITOR-VALUES
- SHOW-FT-OPTIONS
- SHOW-FT-PARTNERS
- SHOW-FT-PROFILE
- SHOW-FT-RANGE

  * see User Guide

Many programs such as spreadsheets, databases, etc., can import data in CSV format. This means that you can use the processing and presentation features of such programs on the CSV outputs of the command listed above.

The field names of the CSV outputs are described in the appendix.

The first line is the header and contains the field names of the respective columns. **Only the field names are guaranteed, not the order of fields in a record.** In other words, the order of columns is determined by the order of the field names in the header line.

One example of a possible evaluation procedure is supplied a template in the Microsoft Excel format under the name $SYSFJAM.FTACCNT.XLT. You will need to first make a binary copy of this template on your PC. The template evaluates a CSV log file by means of an automatically running macro. The result shows the number of inbound and outbound requests and the Kilobytes transferred in each case for all BS2000 users.

5.7 ADD-FT-PARTNER Add remote system to the partner list

Note on usage

User group: FT administrator

Alias name: FTADDPTN

Functional description

The ADD-FT-PARTNER is used to enter a remote system in the partner list of the local system. The network or transport system shouldbe generated beforehand.
Please refer to the appropriate manuals on PDN and BCAM for further information on the generation process. A transport system in accordance with ISO or TCP/IP can be used for generation.

If dynamic partners are permitted then inbound and outbound requests can be processed with partners which are accessed via their addresses and are not defined in the partner list.

You can issue the ADD-FT-PARTNER command for all partner types while the FT system is running (openFT partners, FTAM partners, ftp partners and ADM partner).

You can modify the partner system entry with MODIFY-FT-PARTNER (page 249) and delete it with REMOVE-FT-PARTNER (page 282).

Format

```
ADD-FT-PARTNER / FTADDPTN

 PARTNER-NAME = <name 1..8> / *NONE
,PARTNER-ADDRESS = <text 1..200 with-low>
,SECURITY-LEVEL = *STD / *BY-PARTNER-ATTRIBUTES / <integer 1..100>
,STATE = *PARAMETERS(...)
   *PARAMETERS(...)
     |  OUTBOUND = *ACTIVE(...) / *DEACT
     |       |  *ACTIVE(...)
     |       |      AUTOMATIC-DEACT = *NO / *YES
     |  ,INBOUND = *ACTIVE / *DEACT
,IDENTIFICATION = *STD / <composed-name 1..64> / <c-string 1..64 with-low>
,SESSION-ROUTING-INFO = *NONE / *IDENTIFICATION / <alphanum-name 1..8>
,PARTNER-CHECK = *BY-FT-OPTIONS / *STD / *TRANSPORT-ADDRESS
,TRACE = *BY-FT-OPTIONS / *ON / *OFF
,AUTH-MANDATORY= *NO / *YES
,PRIORITY= *NORMAL / *LOW / *HIGH
,REQUEST-PROCESSING = *STD / *SERIAL
```

Operands

PARTNER-NAME =
Symbolic name of the partner system. It can be freely selected and need only be unique within openFT.

PARTNER-NAME = <name 1..8>
The operand value “name” consists of a maximum of 8 alphanumeric characters and must be unique in the local system. The FT administrator defines this name. This name can be used in the PARTNER parameter in all FT commands in order to address the partner system.

PARTNER-NAME = *NONE
Specifies that the partner is a dynamic partner.

PARTNER-ADDRESS = <text 1..200 with-low>
Address of the partner system. This specifies whether the partner is an openFT or FTAM or FTP or ADM partner. For more information on address specifications see section “Defining partner properties” on page 44.

SECURITY-LEVEL =
Assigns a security level to a remote system.

SECURITY-LEVEL = *STD

If you set this operand to *STD or if you do not enter a value here, a standard security level is assigned to the remote system. This standard security level is defined using the command MODIFY-FT-OPTIONS. You can define a fixed value or specify that the value should be attribute-dependent.

SECURITY-LEVEL = *BY-PARTNER-ATTRIBUTES

If you set this operand to *STD or if you do not enter a value here, a standard security level is assigned to the remote system:

- This setting assigns partners that are authenticated by openFT the security level 10.
- Partners that are known in BCAM (i.e. they are addressed via their BCAM names) are assigned the security level 90.
- All other partners are assigned security level 100.

SECURITY-LEVEL = <integer 1..100>

Must be specified if you wish to assign an individual security level to a specific remote system.

STATE = *PARAMETERS(...)

Controls the status of the partner system, i.e. the settings for file transfer requests issued locally (outbound) and file transfer requests issued remotely (inbound).

OUTBOUND =

Specifies the settings for file transfer requests issued locally to this partner system.

OUTBOUND = *ACTIVE(...)

File transfer requests issued locally to this partner system are processed.

AUTOMATIC-DEACT =

Defines whether cyclical attempts to establish a connection to this partner system are prohibited after a number of attempts by deactivating the partner system.

AUTOMATIC-DEACT = *NO

Failed attempts to establish a connection of this partner system do not result in its deactivation.

AUTOMATIC-DEACT = *YES

Failed attempts to establish a connection of this partner system result in its deactivation. In order to enable file transfer requests issued tocally to this partner system to be executed again subsequently, it must be explicitly activated (with OUTBOUND=*ACTIVE).

OUTBOUND = *DEACT

File transfer requests issued locally to this partner system are initially not processed (not started), but are only placed in the request queue. They are executed only after the partner system has been activated with
MODIFY-FT-PARTNERS ... , STATE=(OUTBOUND=*ACTIVE).

INBOUND =
Specifies the settings for file transfer requests issued remotely, i.e. requests which are issued by this partner system.

INBOUND = *ACTIVE
File transfer requests issued remotely by this partner system are processed.

INBOUND = *DEACT
Synchronous file transfer requests issued remotely by this partner system are rejected. Asynchronous file transfer requests issued remotely by this partner system are stored there and cannot be processed until this partner system is activated with INBOUND=*ACTIVE.

IDENTIFICATION =
Network-wide, unique identification of the openFT instance in the partner system.

IDENTIFICATION = *STD
For openFT and FTADM partners, the partner address or the hostname from the partner address is used as the identification. For FTP and FTAM partners, no identification is set.

IDENTIFICATION = <composed-name 1..64> / <c-string 1..64 with-low>
The network-wide, unique instance ID of the openFT instance in the partner system. This ID is used for authentification of partner systems as of openFT V8.1. It is set by the FT administrator of the partner system (in BS2000 by using MODIFY-FT-OPTIONS IDENTIFICATION=, in Unix systems or Windows systems, by using ftmodo -id). The uniqueness of this ID must be based on something other than case-sensitivity. An instance ID may be comprised of alphanumeric characters or special characters. It is advisable only to use the special characters “.”, “-”, “:” or “%”. The initial character must be alphanumeric or the special character “%”. The “%” character may only be used as an initial character. An alphanumeric character must follow the “.” character.

For more details on allocating instance IDs, please refer to page 55.

With FTAM partners an Application Entity Title can be specified as an identification in the format *n1.n2.n3.n4..mmm*. For details, see the section "Addressing via Application Entity Title" in the openFT User Guide.

No instance identification may be specified for FTP partners.

i You should always specify the instance identification of the partner system explicitly (except in the case of FTAM and FTP partners) and should not use the default value (IDENTIFICATION=*STD).

SESSION-ROUTING-INFO =
If the partner system is only accessible by a go-between instance (for example openFTIF gateway), specify the address information that the gateway instance uses for re-routing here.
This is necessary, for example, for partner systems using openFT for OS/390 and z/OS, dependent on TRANSIT coupling.

SESSION-ROUTING-INFO = *NONE
By default, no specification is required.
The session selector can be specified as a part of the partner address.

SESSION-ROUTING-INFO = *IDENTIFICATION
Connections to the partner are re-routed via a gateway that supports the instance ID as address information.

SESSION-ROUTING-INFO = <alphanum-name 1..8>
Connections to the partner are re-routed via a gateway that supports the specified character string as address information.

PARTNER-CHECK =
Modifies the global settings for the sender check in a partner-specific way. These settings are only valid for named openFT partners that do not work with authentication.
This setting has no meaning for FTAM partners, FTP partners and dynamic partner entries.

PARTNER-CHECK = *BY-FT-OPTIONS
The global settings are valid for the partners.

PARTNER-CHECK = *STD
Disables the expanded sender checking. The transport address of the partner is not checked, even if the expanded sender checking is globally enabled (see the MODIFY-FT-OPTIONS command).

PARTNER-CHECK = *TRANSPORT-ADDRESS
Enables the expanded sender checking. The transport address is checked, even if the expanded sender checking is globally disabled (see the MODIFY-FT-OPTIONS command).
If the transport address under which the partner is reporting does not correspond to the entry in the partner list, the request is rejected.

TRACE =
Trace setting for openFT partner systems. Trace entries are generated only when the FT trace function is activated by an operating parameter (MODIFY-FT-OPTIONS TRACE=*ON).

TRACE = *BY-FT-OPTIONS
The global settings apply for the partner.

TRACE = *ON
The trace function is activated for this partner. However, the trace is only written if the global openFT trace function is also activated (see also the MODIFY-FT-OPTIONS command, TRACE option, SWITCH=*ON). The setting made here takes priority over the setting in the operating parameters for selecting partners for the monitoring function, see the option TRACE=(...,PARTNER-SELECTION=).

i A detailed description of the trace function is provided in the section “Diagnostics” on page 91.

TRACE = *OFF
The trace function is deactivated for this partner.

AUTH-MANDATORY =
Allows you to force the authentication of a named partner.

AUTH-MANDATORY = <u>*NO</u>
Authentication is not forced, i.e. this partner is not restricted with regard to authentication.

AUTH-MANDATORY = *YES
Authentication is forced, i.e. connections to and from this partner are only permitted with authentication.

PRIORITY=
This operand allows you to specify the priority of a partner in respect of processing requests that have the same request priority. This means that the partner priority only applies in the case of requests that have the same request priority, but that are issued to partners with a different partner priority.

PRIORITY = <u>*NORMAL</u>
The partner has normal priority.

PRIORITY = *LOW
The partner has low priority.

PRIORITY = *HIGH
The partner has high priority.

REQUEST-PROCESSING =
You use this option to control whether asynchronous outbound requests to this partner are always run serially or whether parallel connections are permitted.

REQUEST-PROCESSING = *STD
Parallel connections to this partner are permitted.

REQUEST-PROCESSING = *SERIAL
Parallel connections to this partner are not permitted. If multiple file transfer requests to this partner are pending, then they are processed serially. A follow-up request is consequently not started until the preceding request has terminated.

If the ADD-FT-PARTNER command is executed correctly then no message is output.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
35	64	FTR1035	Command only permissible for FT administrator.
43	64	FTR1043	Partner with same attribute already exists in partner list.
44	64	FTR1044	Maximum number of partners exceeded.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section "Command return codes" on page 133

5.7.1 Notes on entering partner systems

The following principles must be adhered to when entering named openFT and FTADM partner systems in the partner list:

- Partner systems are always addressed in the inbound direction via the instance IDs of their openFT instance (the IDENTIFICATION parameter).
- For partners using openFT as of version 8.1, the instance ID is set by the FT administrator of the partner system. Refer to the note in the section "Instance identifications" on page 55.
- For partners using openFT version 8.0 (or earlier), the instance ID has the following format:

  %.<processor>.<entity>

  This enters the address of the main station of the partner system just as it was defined in the partner system or as it was assigned to the partner system by the network administration, see also section "Addressing concept for partners up to openFT V8.0" on page 51.

5.7.2 Sample openFT partner entries

Partner systems via computer-to-computer connection

A partner system that uses openFT V8.1 or later is addressed via its instance ID. This can be obtained from the network administrator or the system administrator of the partner system.

Example 1

A partner system that uses openFT V12.0 for BS2000 and whose symbolic name is *FTBS2* is to be entered in the partner list. Its processor name is *VAR1* and the instance ID is *VAR1.FUSINET.AT*. The appropriate command is as follows:

```
/ADD-FT-PARTNER                                    -
/     PARTNER-NAME=FTBS2,                          -
/     PARTNER-ADDRESS=VAR1,                        -
/     IDENTIFICATION='VAR1.FUSINET.AT'
```

Example 2

The Unix based partner system with the symbolic name *FTUNI2*, on which openFT V8.0 is installed, is to be entered in the partner list. The partner system is connected via computer interconnection. Its processor name is *UNIX2*, which is defined in the Unix system by means of the command fta -p. The corresponding command is:

```
/ADD-FT-PARTNER                                    -
/     PARTNER-NAME=FTUNI2                          -
/     PARTNER-ADDRESS=UNIX2,                       -
/          IDENTIFICATION='%.UNIX2.$FJAM'
```

Example 3

The partner system *FTSIE1* with openFT V10.0 for Unix systems is accessed via TCP/IP with the IP address 123.123.45.67. The FT administrator of the partner system has correspondingly assigned it the instance ID %ip123.123.45.67. The processor name *UNIX9* is assigned to the partner system and it uses the default port number for openFT. The port number is defined in the Unix system by means of the openFT operating parameter.

```
/ADD-FT-PARTNER                                         -
/     PARTNER-NAME=FTSIE1,                              -
/     PARTNER-ADDRESS=UNIX9,                  -
/        IDENTIFICATION='%ip123.123.45.67'
```

Partner systems via ISO

If the partner system is connected via ISO, the differences relate solely to the generation of the transport system. The partner entry using ADD-FT-PARTNER occurs as described in the section "Partner systems via computer-to-computer connection" on page 143.

5.7.3 Example for entering a remote administration server

Example

The partner system SERVER11 with openFT V11 for Unix systems is a remote administration server. The default port number (11000) is to be used for remote administration. The partner address is to be used for identification.

```
/ADD-FT-PARTNER                                                    -
/     PARTNER-NAME=ADMINSRV,                                       -
/     PARTNER-ADDRESS=FTADM://SERVER11
```

5.7.4 Sample FTAM partner entries

Example 1

The FTAM partner *RITTER* is to be entered in the partner list. At BCAM generation, this system was assigned the processor name *BURGHOF1*. The transport selector is *KUNIBERT*, the session selector is *SESSION1* and the presentation selector is *FTAM*.

```
/ADD-FT-PARTNER RITTER,FTAM://BURGHOF1:.KUNIBERT.SESSION1.FTAM
```

Positional operands were used in this statement. This is why the keywords are omitted.

If the partner requires a transport selector which is not in TRANSDATA format (8 character name in EBCDIC, filled with blanks if necessary), this must be defined in BCAM.

If the partner uses, for example, the 6-character transport selector TSKUNI in ASCII format, the BCMAP command must be as follows:

```
/BCMAP FUNCT=DEFINE,SUBFUNCT=GLOBAL,                         -
/      NAME=KUNIBERT,                                        -
/      ES=BURGHOF1,                                          -
/      PTSEL-I=(6,x‘54534B554E49‘)
```

Example 2

Since some FTAM implementations respond with another address during connection setup, openFT for BS2000 requires a further entry defining the sender address of the partner for the purpose of checking the sender for this partner.

The partner responds with the FTAM1 transport selector, the SESSION2 session selector and the FTAM presentation selector (all in ASCII code):

```
/ADD-FT-PARTNER                                                     -
/    PARTNER-NAME=RITTERXX,                                         -
/    PARTNER-ADDRESS=FTAM://BURGHOF1:.X‘4654414D31404040‘.SESSION2.FTAM,-
/    STATE = *DEACT
```

The relevant BCMAP command must be:

```
/BCMAP FUNCT = DEFINE,SUBFUNCT = GLOBAL,        -
/      NAME = KUNI,                             -
/      ES = BURGHOF1,                           -
/      PTSEL-I = (5,X‘4654414D31‘)
```

Example 3

FTAM connection between openFT for BS2000 <-> openFT for Windows (openFT as of V11.0)

The FTAM partner WINDOWS is to be entered in the partner list. The default transport selector has the name $FTAM in TRANSDATA format; the computer has the processor name WINDOWS2.

```
/ADD-FT-PARTNER WINDOWS,FTAM://WINDOWS2
```

A BCMAP command is no longer necessary for this connection!

Example 4

FTAM link: openFT for BS2000 <-> openFT for Windows (openFT up to V10.0)

The FTAM partner WINDOWS is to be entered in the partner list. At BCAM generation, this system was assigned the processor name WINDOWS1. The transport selector is SNI-FTAM in ASCII code and the port number 4800.

```
/ADD-FT-PARTNER WINDOWS,FTAM://WINDOWS1:.SNI-FTAM
```

The relevant BCMAP command must be:

```
/BCMAP FUNCT = DEFINE,SUBFUNCT = GLOBAL,        -
/      NAME = SNI-FTAM,                         -
/      ES = WINDOWS1,                           -
/      PTSEL-I = (8,X‘534E492D4654414D‘),       -
/      PPORT# = 4800
```

5.7.5 Examples for entering FTP partners

Example 1

The FTP partner FTP1 with the IP address 192.168.20.10 is to be entered in the partner list. It is accessed via the default port 21.

```
/ADD-FT-PARTNER                                  -
/       PARTNER-NAME=FTP1,                       -
/       PARTNER-ADDRESS=FTP://%ip192.168.20.10
```

Example 2

The FTP partner FTP2 with the host name UX1 is to be entered in the partner list. It is accessed via port 1234.

```
/ADD-FT-PARTNER                             -
/       PARTNER-NAME=FTP2,                  -
/       PARTNER-ADDRESS=FTP://UX1:1234
```

5.8 CANCEL-FILE-TRANSFER Cancel file transfer requests

Note on usage

User group: FT user and FT administrator

Alias names: CNFT / NCANCEL / FTCANREQ

Functional description

The CANCEL-FILE-TRANSFER command can be used to cancel a file transfer request or to abort the file transfer. The FT system deletes from the request queue the file transfer request that corresponds to the specified selection criteria and, if necessary, aborts the associated file transfer.

The following features apply to this command:

- FT requests submitted either in the local or the remote system can be canceled.
- A single command can be used to cancel several FT requests simultaneously.
- The FT requests to be canceled can be selected using different selection criteria.
- As FT administrator you can cancel requests from any user, whereas an FT user can only cancel those FT requests that he/she owns.
- As FT Administrator you can also fully and unconditionally cancel a selected request and remove it from the request file. “Unconditional” means that, if necessary, the request can be cancelled without any negotiation with the corresponding partner system. In this way, you can clear the request file of requests which are no longer recognized in the partner system or for which there is no longer any connection to the partner system.

WARNING!
If not used carefully, this function can result in inconsistencies in the request files of the corresponding partner systems. Under certain circumstances these inconsistencies may cause baffling error messages (SYSTEM ERROR) and “dead requests” in the partner system request files. It should therefore only be used in exceptional circumstances and after a suitable period has elapsed.

When a request is canceled, it is only deleted completely from the request file after it has been deleted from the request file in the remote system.

Format

```
CANCEL-FILE-TRANSFER / CNFT / NCANCEL / FTCANREQ
--------------------------------------------------------------------------------
 TRANSFER-ID = *ALL/ <integer 1..2147483647> (FORCE-CANCELLATION = *NO / *YES)
,SELECT = *OWN / *PARAMETERS(...)
   *PARAMETERS(...)
     |  OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
     | ,INITIATOR = (*LOCAL, *REMOTE) / list-poss(2): *LOCAL / *REMOTE
     | ,PARTNER = *ALL / <text 1..200 with-low>
     | ,FILE-NAME = *ALL / <filename 1..54> / <c-string 1..512 with-low> /
     |                  *LIBRARY-ELEMENT(...) /  *POSIX(NAME = <posix-pathname 1..510>) /
     |                  *PUBSET(PUBSET = <cat-id 1..4>)
     |     *LIBRARY-ELEMENT(...)
     |       |  LIBRARY = *ALL / <filename 1..54>
     |       | ,ELEMENT = *ALL / <filename 1..64 without-gen-vers>(...) /
     |       |                 <composed-name 1..64 with-under>(...)
     |       |     <filename>(...) / <composed-name>(...)
     |       |          |  VERSION = *ALL / <text 1..24>
     |       | ,TYPE = *ALL / <name 1..8>
     | ,MONJV = *NONE / <filename 1..54 without-gen-vers>
     | ,JV-PASSWORD = *NONE / <c-string 1..4> / <x-string 1..8> /
     |                        <integer -2147483648..2147483647> / *SECRET
```

Operands

TRANSFER-ID =
Transfer ID of the FT request to be canceled.

TRANSFER-ID = *ALL
FT users can only delete FT requests of their own ID using this entry. FT administrators can delete all current FT requests that access the system.

TRANSFER-ID = <integer 1..2147483647>
Request identification which was communicated to the local system in the FT request confirmation. The associated FORCE-CANCELLATION parameter is available only to the FT administrator. It is used for an **unconditional** request cancellation.

TRANSFER-ID = <integer 1..2147483647>(FORCE-CANCELLATION = *NO)
NO is the default value. The request is removed from the request file following negotiation with the partner system.

TRANSFER-ID = <integer 1..2147483647>(FORCE-CANCELLATION = *YES)
The request is removed from the request file without negotiation with the partner system. This specification is only possible for an FT administrator who has previously attempted to cancel the request with CANCEL-FILE-TRANSFER <transfer-id> (FORCE-CAN=*NO).

SELECT =
Contains selection criteria for FT requests to be canceled. A request is canceled if it satisfies all the specified criteria.

SELECT = *OWN
Cancels all FT requests associated with the own user ID and the specified TRANSFER-ID.

SELECT = *PARAMETERS(...)

OWNER-IDENTIFICATION =
Designates the owner of the FT requests.

OWNER-IDENTIFICATION = *OWN
Cancels only the FT requests under the user's own ID.

OWNER-IDENTIFICATION = *ALL
Cancels FT requests under all user IDs. Only the administrator can use this entry.

OWNER-IDENTIFICATION = <name 1..8>
Specifies a particular user ID whose FT requests are to be canceled.

INITIATOR =
Initiator of the FT requests to be canceled.

INITIATOR = (*LOCAL,*REMOTE)
Cancels FT requests in the local system and in remote systems.

INITIATOR = *LOCAL
Cancels FT requests issued in the local system.

INITIATOR = *REMOTE
Cancels FT requests issued in remote systems.

PARTNER =
Cancels FT requests that were to be executed with a specific partner system.

PARTNER = *ALL
The name of the partner system is not used as a selection criterion to determine the FT requests to be canceled.

PARTNER = <text 1..200 with-low>
The FT requests that were to be executed with this partner are to be canceled. You can specify either the name of the partner system from the partner list or the address of the partner system,.

FILE-NAME =
Cancels all FT requests in the local system that access this file, this pubset or this library element whether as a send file or receive file. The file name or library member name must be specified exactly as it appears in the file transfer request.

FILE-NAME = *ALL
The file name is not used as a selection criterion to determine the FT requests to be canceled.

FILE-NAME = <filename 1..54> / <c-string 1..512 with-low> /
***POSIX(NAME = <posix-pathname 1..510>)**
Cancels FT requests in the local system that access this file.

FILE-NAME = *PUBSET(PUBSET = <cat-id 1..4>)
Deletes all FT requests that have locked files on the specified pubset. Only the FT administrator can use this specification.

FILE-NAME = *LIBRARY-ELEMENT(...)
Cancels FT requests that access library members in the local system.

LIBRARY =
Selects the library concerned.

LIBRARY = *ALL
The library name is not used as a selection criterion to determine the FT requests to be canceled.

LIBRARY = <filename 1..54>
FT requests that access this library are to be canceled.

ELEMENT =
Selects the library concerned.

ELEMENT = *ALL
The name of the library member is not a selection criterion to determine the FT requests to be canceled.

ELEMENT = <filename 1..64 without-gen-vers>(...) /
<composed-name 1..64 with-under>(...)
Name of the library member concerned.

VERSION =
Version of the library member.

VERSION = *ALL
The version of the library member is not a selection criterion for the FT requests to be canceled.

VERSION = <text 1..24>
Only FT requests that access this version of the library member are to be canceled.

TYPE =
Type of the library member concerned.

TYPE = *ALL
The type of library member is not used as a selection criterion to determine the FT requests to be canceled.

TYPE = <name 1..8>
Only FT requests that access library members of this type are to be canceled.

MONJV =
If appropriate, selects the specific FT request that is being monitored by this job variable.

MONJV = *NONE
A job variable is not selected as a selection criterion to cancel the file transfer.

MONJV = <filename 1..54 without-gen-vers>
The FT monitored by this job variable is to be canceled.

JV-PASSWORD =
If required, specifies the password needed to access the job variable.
If you have already notified the system of the password with the BS2000 command ADD-PASSWORD, you do not have to specify JV-PASSWORD.

JV-PASSWORD = *NONE
The job variable is not password-protected.

JV-PASSWORD = <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
This password is required to access the job variable.

JV-PASSWORD = *SECRET
The system issues the request to enter the password. However, input is not displayed on the screen.

The specification of more than one selection criteria in the CANCEL-FILE-TRANSFER command may result in a file transfer request being “overdefined” (e.g. by entries for TRANSFER-ID and MONJV). If all selection criteria for a request apply, the job is canceled. If not all selection criteria for a request apply, it is not canceled.
If the specified criteria conflict, the CANCEL-FILE-TRANSFER command is acknowledged with the following message:

```
%  FTR0504 No requests available for the selection criteria
```

In such a case there is no jump to the next SET-JOB-STEP in procedures as no error has occurred.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	There are no requests that meet the specified selection criteria.
32	32	CMD0221	Request rejected. Internal error. Job variable not accessible.
33	32	CMD0221	Request rejected. Internal error.
36	32	CMD0221	Request rejected. Request data inconsistent.
82	32	CMD0221	Internal error. Job variable not accessible.
83	32	CMD0221	Internal error.
36	64	FTR1036	User not authorized for other user IDs.
38	64	FTR1038	Request is in the termination phase and can no longer be cancelled.
47	64	FTR1047	Request with the specified transfer ID could not be found.
226	64	FTR2226	Job variable contents inconsistent.
227	64	FTR2227	Job variable not in use by openFT.
228	64	FTR2228	Job variable not found.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

If more than one job wurde be deleted by a CANCEL-FILE-TRANSFER command, the following prompt appears:

```
%  FTR0560 Cancel all specified requests? Reply (y=yes: n=no)
```

With `N` the deletion request can be cancelled.

5.9 CREATE-FT-INSTANCE Create a new openFT instance or activate an unloaded openFT instance

Note on usage

User group: FT administrator

Functional description

Using this CREATE-FT-INSTANCE command, you create a new administration entry for an instance and load the instance. You can optionally create the instance in such a manner that when the subsystem FT is started, openFT is also automatically started in this instance a START-FT / FSTART command is no longer necessary). In addition, the command reactivates or reloads an instance that was unloaded using DELETE-FT-INSTANCE.

In addition to the default instance, you can define up to 16 other instances, see also the section “Using openFT in a HIPLEX cluster” on page 88.

Format

CREATE-**FT**-**INST**ANCE
NAME = <alphanum-name 1..8> ,**CON**FIG-**USER**ID = <text 1..15> ,**AUTO**MATIC-**START** = *OFF / *ON

Operands

NAME = <alphanum-name 1..8>
The name of the openFT instance that is to be created. This name must be identical on all of the computers on which this instance is to be used.

CONFIG-USERID = <text 1..15>
The file name prefix of the openFT instance variable files. The prefix must consist of a catalog name and a USER-ID. This USER-ID is designated as the configuration user ID of the instance.

AUTOMATIC-START=
This is specified if an automatic start of openFT is to occur within an instance, after loading the instance.

AUTOMATIC-START = *OFF
openFT is not started after loading the instance.

AUTOMATIC-START = *ON
After each loading of the instance, a START-FT command is implicitly executed in this instance. By doing this, it is possible to immediately work with openFT after loading. All the components which are available to a standard instance are also started, such as, for example openFT-AC, openFT-FTAM and openFT-FTP.

Command return codes

(SC2)	SC1	Maincode	Meaning
195	1	CMD0202	Invalid parameter.
83	32	CMD0221	Internal error.
22	64	FTR1022	Instance already exists.
23	64	FTR1023	Maximum number of instances exceeded.
2	0	FTR1028	Config user ID not accessible.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.10 CREATE-FT-KEY-SET Create a key pair set

Note on usage

User group: FT administrator

Alias name: FTCREKEY

Functional description

Using this CREATE-FT-KEY-SET command, you create a key pair for authenticating your openFT instance in partner systems (RSA procedures). The key pair consists of a private key, administered internally by openFT, and a public key.

Public keys are stored on the configuration user ID of the FT instance (default: $SYSFJAM) under the name:

SYSPKF.R<key reference>.L<key length>

The key reference is a numerical designator for the version of the key pair. The key length is 768 or 1024 or 2048. The three key lengths are always generated. The public key files are text files which are created in the character code of the respective operating system, i.e. EBCDIC.DF04-1 for BS2000, IBM1047 for z/OS, ISO8859-1 for Unix systems and CP1252 for Windows systems.

In a file SYSPKF.COMMENT on the configuration user ID of the openFT instance you can store comments, which are written in the first lines of the public key files when a key pair set is created. Such comments could be, for example, the communications partner and the telephone number of the FT administrator on duty. The lines in the SYSPKF.COMMENT file may be a maximum of 78 characters long.

So that your openFT instance can be authenticated by partner systems (using openFT as of version 8.1), the public key file must be transported to the partners via a reliable path and re-coded if necessary (see section “Authentication” on page 53).

In order to make an authorized update of the key pair sets, openFT supports up to three key pair sets at a time.

The most current key pair is used for delivering the session key for encrypting user data and request description data. If there is no key pair set, work proceeds without encryption.

Format

CREATE**-FT-KEY**-SET / **FTCREKEY**

Without operands

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
87	32	CMD0221	No space left on device for internal files.
29	64	FTR1029	Maximum number of key pairs exceeded.
35	64	FTR1035	Command only permissible for FT administrator.

SC1/2 = Subcode 1/2 in decimal-notation
For additional information see section “Command return codes” on page 133

5.11 CREATE-FT-PROFILE Create admission profile

Note on usage

User group: FTAC user and FTAC administrator

A prerequisite for using this command is the use of openFT-AC.

Functional description

All FTAC users can use CREATE-FT-PROFILE to set up their own admission profiles under their user IDs. Users must activate admission profiles predefined by the FTAC administrator with MODIFY-FT-PROFILE (see page 257ff) before they can be used. Profiles predefined by the FTAC administrator may be used immediately if the FTAC administrator also possesses the TSOS privilege .

The FTAC administrator can use CREATE-FT-PROFILE to create admission profiles for each user. It is necessary to distinguish between three cases:

– The FTAC administrator possesses the TSOS privilege . He/She can then create profiles for other user IDs without restriction which are available for immediate use if they are complete. If the FTAC administrator specifies *NOT-SPECIFIED for ACCOUNT or PASSWORD in the USER-ADMISSION operand, the profiles are not locked, but they cannot be used, either

– If the FTAC administrator does not possess the TSOS privilege but specifies ACCOUNT and PASSWORD in the USER-ADMISSION parameter, then he/she may also assign a TRANSFER-ADMISSION for the profile. However, this functions only for as long as the current password for the user ID corresponds to the one defined in the profile.

– If the FTAC administrator does not possess the TSOS privilege and also does not specify the user's account number and password, then he/she may not define any TRANSFER-ADMISSION in the profile. In this case, the user must then assign the profile a TRANSFER-ADMISSION with the MODIFY-FT-PROFILE command, and the specifications for the USER-ADMISSION must, if necessary, be complemented.

  Example

  The FTAC administrator creates an admission profile for user USER1. In doing so he/she specifies only the user ID for the USER-ADMISSION, but not the account number and password. In this case the FTAC administrator may also not specify a TRANSFER-ADMISSION.

```
CR-FT-PROF NAME=HISPROF2,TRANS-ADM=*NOT-SPECIFIED, -
USER-ADM=(USER1,*NOT-SPECIFIED,*NOT-SPECIFIED)
```

– It is possible to create an admission profile for "pre-processing" or "post-processing". To do this, the FILE-NAME operand must start with the pipe symbol '|'. After this has been done, one or more BS2000 commands can be specified. For detailed information refer to the section "Preprocessing and postprocessing" in the User Guide.

Format

(part 1 of 2)

```
CREATE-FT-PROFILE

 NAME = *STD / <alphanum-name 1..8>
,PASSWORD = *NONE / <c-string 1..8 with-low> / <x-string 1..16> / *SECRET
,TRANSFER-ADMISSION = *NOT-SPECIFIED / <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) /
                       <x-string 15..64>(...) / *SECRET
   <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...)
        VALID = *YES / *NO
       ,USAGE = *PRIVATE / *PUBLIC
       ,EXPIRATION-DATE = *NOT-RESTRICTED / <date 8..10>
,PRIVILEGED = *NO / *YES
,IGNORE-MAX-LEVELS = *NO / *YES / *PARAMETERS(...)
   *PARAMETERS(...)
        OUTBOUND-SEND = *NO / *YES
       ,OUTBOUND-RECEIVE = *NO / *YES
       ,INBOUND-SEND = *NO / *YES
       ,INBOUND-RECEIVE = *NO / *YES
       ,INBOUND-PROCESSING = *NO / *YES
       ,INBOUND-MANAGEMENT = *NO / *YES
,USER-ADMISSION = *OWN / *PARAMETERS(...)
   *PARAMETERS(...)
        USER-IDENTIFICATION = *OWN / <name 1..8>
       ,ACCOUNT = *OWN / *FIRST / *NOT-SPECIFIED / *NONE / <alphanum-name 1..8>
       ,PASSWORD = *OWN / *NOT-SPECIFIED / <c-string 1..8> / <c-string 9..32> / <x-string 1..16> /
                   *NONE / *SECRET
,INITIATOR = (*LOCAL, *REMOTE) / list-poss(2): *LOCAL / *REMOTE
,TRANSFER-DIRECTION = *NOT-RESTRICTED / *FROM-PARTNER / *TO-PARTNER
,PARTNER = *NOT-RESTRICTED / list-poss(50): <text 1..200 with-low>
,MAX-PARTNER-LEVEL = *NOT-RESTRICTED / <integer 0..100>
```

(part 2 of 2)

```
,FILE-NAME = *NOT-RESTRICTED / <filename1..54 > / <c-string 1..512 with-low> /
             *EXPANSION(...) / *LIBRARY-ELEMENT(...) / *POSIX(NAME=<posix-pathname 1..510>

   ,*EXPANSION(...)
      PREFIX = <filename 1..53> / <partial-filename 2..53> / <c-string 1..511 with-low>

   *LIBRARY-ELEMENT(...)
      LIBRARY = *NOT-RESTRICTED / <filename 1..54> / *EXPANSION(...)
         *EXPANSION(...)
            PREFIX = <filename 1..53> / <partial-filename 2..53>
     ,ELEMENT = *NOT-RESTRICTED / <composed-name 1..64 with-under>(...) / *EXPANSION(...)
         <composed-name 1..64 with-under>(...)
            VERSION = *STD / <text 1..24>
         *EXPANSION(...)
            PREFIX = <composed-name 1..63 with-under> / <partial-filename 2..63>
     ,TYPE = *NOT-RESTRICTED / <name 1..8>

,FILE-PASSWORD = *NOT-RESTRICTED / *NONE / <c-string 1..4> / <x-string 1..8> /
                 <integer -2147483648...2147483647> / *SECRET

,PROCESSING-ADMISSION = *SAME / *NOT-RESTRICTED / *PARAMETERS(...)

   *PARAMETERS(...)
      USER-IDENTIFICATION = *SAME / *NOT-RESTRICTED / <name 1..8>
     ,ACCOUNT = *SAME / *NOT-RESTRICTED / *NONE / <alphanum-name 1..8>
     ,PASSWORD = *SAME / *NOT-RESTRICTED / *NONE / <c-string 1..8> /
                 <c-string 9..32> / <x-string 1..16> / *SECRET

,SUCCESS-PROCESSING = *NOT-RESTRICTED / *NONE / <c-string 1..1000 with-low> / *EXPANSION(...)

   *EXPANSION(...)
      PREFIX = *NOT-RESTRICTED / <c-string 1..999 with-low>
     ,SUFFIX = *NOT-RESTRICTED / <c-string 1..999 with-low>

,FAILURE-PROCESSING = *NOT-RESTRICTED / *NONE / <c-string 1..1000 with-low> / *EXPANSION(...)

   *EXPANSION(...)
      PREFIX = *NOT-RESTRICTED / <c-string  1..999 with-low>
     ,SUFFIX = *NOT-RESTRICTED / <c-string 1..999 with-low>

,WRITE-MODE =  *NOT-RESTRICTED / *NEW-FILE / *REPLACE-FILE / *EXTEND-FILE

,FT-FUNCTION = *NOT-RESTRICTED / list-poss(5): *TRANSFER-FILE / *MODIFY-FILE-ATTRIBUTES /
               *READ-DIRECTORY / *FILE-PROCESSING / *REMOTE-ADMINISTRATION

,USER-INFORMATION = *NONE / <c-string 1..100 with-low>

,DATA-ENCRYPTION = *NOT-RESTRICTED / *NO / *YES
```

Operands

NAME = <alphanum-name 1..8>
With NAME, the admission profile is given a name. This name must be unique among all admission profiles on the user ID specified in USER-ADM. If an admission profile with this name already exists, FTAC rejects the command with the message:

```
FTC0100 FT profile already exists
```

The command SHOW-FT-PROFILE (see page 372ff) can be used to view the already existing names. To obtain this information, the command SHOW-FT-PROFILE can be entered and a user ID must be specified.

NAME = *STD
Creates a default admission profile for the user ID. You must specify *NOT-SPECIFIED as the transfer admission, because a default admission profile in a request is addressed using the user ID and password. You must not specify the parameters VALID, USAGE and EXPIRATION-DATE for a default admission profile.

PASSWORD =
FTAC password which authorizes you to issue FTAC commands on your user ID, if such a password was defined in your admission set.

PASSWORD = *NONE
No FTAC password is required.

PASSWORD = <c-string 1..8 with-low> / <x-string 1..16>
This FTAC password is required.

PASSWORD = *SECRET
The system prompts you to input the password. However, the password does not appear on the screen.

TRANSFER-ADMISSION =
With TRANSFER-ADMISSION, you define transfer admission. If this transfer admission is entered in an FT request instead of the LOGON admission, then the access rights are valid which are defined in this admission profile. This transfer admission must be unique in the entire openFT system, so that there is no conflict with other transfer admissions which other FTAC users have defined for other access rights. When the transfer admission which you have selected has already been used, then FTAC rejects the command with the message:

```
FTC0101 Transfer admission already exists
```

The FTAC administrator can also assign a transfer admission when he/she creates an admission profile for a user ID. If the FTAC administrator possesses no TSOS admission, he/she must also enter the complete USER-ADMISSION for the user ID in question (USER-IDENTIFICATION, ACCOUNT and PASSWORD).

TRANSFER-ADMISSION = *NOT-SPECIFIED
This entry is used to set up a profile without transfer admission. If the profile is not a default admission profile, it is locked until you specify a valid transfer admission or the owner specifies a valid transfer admission.

TRANSFER-ADMISSION = <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...)
The character string must be entered as the transfer admission in the transfer request. The alphanumeric entry is always stored in lower-case letters.

VALID = *YES
The transfer admission is valid.

VALID = *NO
The transfer admission is not valid. With this entry, users can be denied access to the profile.

USAGE = *PRIVATE
Access to your profile is denied for security reasons, when someone with another user ID attempts a second time to specify the TRANSFER ADMISSION which has already been used by you.

USAGE = *PUBLIC
Access to your profile is not denied if another user happens to “discover” your TRANSFER-ADMISSION. “Discovery” means that another user ID attempted to specify the same TRANSFER ADMISSION twice. This is rejected for uniqueness reasons.

EXPIRATION-DATE = *NOT-RESTRICTED
The use of this transfer admission is not restricted with respect to time.

EXPIRATION-DATE = <date 8..10>
Date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2012-03-31 or 12-03-31 for March 31, 2012. The use of the transfer admission is only possible until the given date.

TRANSFER-ADMISSION = *SECRET
The system prompts you to input the transfer admission. However, this does not appear on the screen. The operands VALID, USAGE and EXPIRATION-DATE can also be secretly entered in this case.

PRIVILEGED =
The FTAC administrator can privilege the profile. FT requests which are processed with a privileged admission profile are not subject to the restrictions which are set for MAX-ADM-LEVEL (see page 308) in the admission set.

PRIVILEGED = *NO
The admission profile is not privileged.

PRIVILEGED = *YES
The admission profile is privileged.

Only the FTAC administrator can use this entry.

IGNORE-MAX-LEVELS =
You can determine for which of the six basic functions the restrictions of the admission set should be ignored. The user's MAX-USER-LEVELS can be exceeded in this way. The MAX-ADM-LEVELS in the admission set can only be effectively exceeded with an admission profile which has been designated as privileged by the FTAC administrator. The FTAC user can set up an admission profile for himself/herself for special tasks (e.g. sending a certain file to a partner system with which he/she normally is not allowed to conduct a file transfer), which allows him/her to exceed the admission set. This profile must be explicitly given privileged status by the FTAC administrator.
If you enter IGNORE-MAX-LEVELS=*YES, the settings for **all** the basic functions are ignored. If you wish to ignore the admission set for **specific** basic functions, you need to do this with the operands explained later in the text.
The following table shows which partial components of the file management can be used under which conditions:

Inbound file management function	**Setting in admission set/extension in profile**
Show file attributes	Inbound sending (IBS) permitted
Modify file attributes	Inbound receiving (IBR) **and** Inbound file management (IBF) permitted
Rename files	Inbound receiving (IBR) **and** Inbound file management (IBF) permitted
Delete files	Inbound receiving (IBR) permitted **and** write rule = overwrite in profile
Show directories	Inbound file management (IBF) permitted **and** direction = to partner in profile
Create, rename, delete directories	Inbound file management (IBF) permitted **and** direction = from partner in profile

IGNORE-MAX-LEVELS = *NO
FT requests which are processed with the admission profile are subject to the restrictions of the admission set.

IGNORE-MAX-LEVELS = *YES
*YES allows you to communicate with partner systems whose security level exceeds the specifications of the admission set. Unless you have a privileged profile, you can only exceed the MAX-USER-LEVELS and not the MAX-ADM-LEVELS in the admission set. You must respect the restrictions defined in the admission set by the FTAC administrator. The SHOW-FT-ADMISSION-SET command provides information on the entries made by the FTAC administrator (see example on page 308). This includes information about the current MAX-USER-LEVELS and MAX-ADM-LEVELS settings.

IGNORE-MAX-LEVELS = *PARAMETERS(...)
The following operands can be used to selectively deactivate the default settings for the individual basic functions.

OUTBOUND-SEND = <u>*NO</u>
The maximum security level which can be reached with the basic function “outbound send” is determined by the admission set.

OUTBOUND-SEND = *YES
For the basic function “outbound send”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

OUTBOUND-RECEIVE = <u>*NO</u>
The maximum security level which can be reached with the basic function “outbound receive” is determined by the admission set.

OUTBOUND-RECEIVE = *YES
For the basic function “outbound receive”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

INBOUND-SEND = <u>*NO</u>
The maximum security level which can be reached with the basic function “inbound send” is determined by the admission set.

INBOUND-SEND = *YES
For the basic function “inbound send”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The same applies to the partial component “display file attributes” of the basic function “inbound file management”.

INBOUND-RECEIVE = <u>*NO</u>
The maximum security level which can be reached with the basic function “inbound receive” is determined by the admission set.

INBOUND-RECEIVE = *YES
You can disregard your settings for “inbound receive” in the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The same applies to the partial components of the basic function “inbound file management”:

– delete files, as long as the file attributes are set accordingly,
– modify file attributes, if the basic function “inbound file management” was admitted in the admission set or in the admission profile.

INBOUND-PROCESSING = <u>*NO</u>
The maximum security level which can be reached with the basic function “inbound follow-up processing” is determined by the admission set.

INBOUND-PROCESSING = *YES
For the basic function “inbound follow-up processing”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

INBOUND-MANAGEMENT = *NO
The maximum security level which can be reached with the basic function “inbound file management” is determined by the admission set.

INBOUND-MANAGEMENT = *YES
For the basic function “inbound file management”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The partial component “modify file attributes” of the basic function “inbound file management” only functions if the basic function “inbound receive” was admitted in the admission set or admission profile.

USER-ADMISSION =
USER-ADMISSION specifies the user ID under which the profile is saved. FT requests which work with this admission profile access the given user ID in the local system.
As FTAC user you can specify only your own user ID here.
If, as FTAC administrator, you create the admission profile for a user, you cannot generally specify neither ACCOUNT nor PASSWORD in the USER-ADMISSION operand (since these should be known only to the user in question). These specifications must be entered by the user by means of MODIFY-FT-PROFILE before the profile can actually be used.
As FTAC administrator you can create a profile which is available for immediate use, i.e. a profile with the TRANSFER-ADMISSION defined, only if you specify the USER-ADMISSION with ACCOUNT and PASSWORD or if you also possess the TSOS privilege. For ACCOUNT= you can also specify *FIRST or *NONE.

USER-ADMISSION = *OWN
For USER-IDENTIFICATION and ACCOUNT, the specifications are taken from the current LOGON authorization. A possible BS2000 password is only taken from your LOGON authorization when an FT request accesses the admission profile. This specification consequently generates a profile in the current user ID.

USER-ADMISSION = *PARAMETERS(...)
Specifies the individual components of the user ID.
This allows you to keep FT requests which use this admission profile under an account number, for example. Or, a password can be set in the admission profile. FT requests which use this admission profile will then only function if LOGON password corresponds to the preset password.

USER-IDENTIFICATION =
User ID in BS2000.

USER-IDENTIFICATION = *OWN
The user ID is taken from the current LOGON authorization.

USER-IDENTIFICATION = <name 1..8>
User ID to which the profile should belong.As FTAC administrator you may also specify foreign user IDs.

ACCOUNT =
Account number under which an FT request is to be kept when it uses this admission profile.

ACCOUNT = *OWN
The account number is taken from the current LOGON authorization.

ACCOUNT = *FIRST
The first account number assigned to the home pubset of the specified USER-IDENTIFICATION at the time the profile is used in the system is used for account assignment in the case of transfer requests. If the ID’s account number changes, the profile does not have to be modified.

ACCOUNT = *NOT-SPECIFIED
No account number is defined.
The account number is first entered by the owner of the admission profile. This function allows the FTAC administrator to create profiles for foreign user IDs whose account number he/she does not know.

ACCOUNT = *NONE
The account number is used which is defined as the default account number of the user ID specified in the USER-IDENTIFICATION at the time the admission profile is used.

ACCOUNT = <alphanum-name 1..8>
An FT request should be kept under the account number specified when it accesses this admission profile. You can enter any account number which belongs to the user ID specified in the USER-IDENTIFICATION.

PASSWORD =
BS2000 password which an FT request should use when it works with this admission profile.

PASSWORD = *OWN
When an FT request refers to this admission profile, FTAC uses the BS2000 password valid for the specified USER-IDENTIFICATION at that moment. This prevents you from having to modify the admission profile if the BS2000 password is changed.

PASSWORD = *NOT-SPECIFIED
The password will be entered by the owner of the admission profile. This function allows the FTAC administrator to create profiles for foreign user IDs whose access data he/she does not know.

PASSWORD = *NONE
No password is required for the user ID specified in the USER-IDENTIFICATION.

PASSWORD = <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
When an FT request accesses the admission profile, the password specified is compared with the current LOGON password. If the two do not correspond, the FT request is rejected.

PASSWORD = *SECRET
The system prompts you to enter the password. The entry does not appear on the screen.

INITIATOR =
Determines if initiators from local and/or remote systems are permitted to use this admission profile for their FT requests.

INITIATOR = (*LOCAL,*REMOTE)
This admission profile may be used by initiators from local and remote systems.

INITIATOR = *REMOTE
This admission profile may only be used for FT requests by initiators from remote systems.

INITIATOR = *LOCAL
This admission profile may only be used for FT requests by initiators from the local system.

TRANSFER-DIRECTION =
Determines which transfer direction may be used with this admission profile. The transfer direction is always determined from the system in which the admission profile was defined.

TRANSFER-DIRECTION = *NOT-RESTRICTED
With this admission profile, files can be transferred to and from a partner system.

TRANSFER-DIRECTION = *FROM-PARTNER
With this admission profile, files can only be transferred from a partner system to your system. It is not possible to display file attributes/directories (partial components of “inbound file management”).

TRANSFER-DIRECTION = *TO-PARTNER
With this admission profile, files can only be transferred from your system to a partner system. It is not possible to modify file attributes or delete files (partial components of “inbound file management”).

PARTNER =
Specifies that this admission profile is to be used only for FT requests which are processed by a a certain partner system.

PARTNER = *NOT-RESTRICTED
The range of use for this admission profile is not restricted to FT requests with certain partner systems.

PARTNER = list-poss(50): <text 1..200 with-low>
The admission profile only permits those FT requests which are processed with the specified partner systems. A maximum of 50 partner names can be specified. The total length of all the partners may not exceed 1000 characters. You may specify the name from the partner list or the address of the partner system, see also section "Defining partner properties" on page 44. It is recommended, to use the name from the partner list. The format shown in the long form of the logging output provides an indication of how a partner address should be entered in an FTAC profile.

MAX-PARTNER-LEVEL =
A maximum security level can be specified. The admission profile will then only permit those FT requests which are processed with partner systems which have this security level or lower.
MAX-PARTNER-LEVEL works in conjunction with the admission set. When non-privileged admission profiles are used, the access check is executed on the basis of the smallest specified value.

MAX-PARTNER-LEVEL = *NOT-RESTRICTED
If FT requests are processed with this admission profile, then the highest accessible security level is determined by the admission set.

MAX-PARTNER-LEVEL = <integer 0..100>
All partner systems which have this security level or lower can be communicated with.

i When you set MAX-PARTNER-LEVEL=0, you prevent access to the admission profile (for the moment). No FT requests can be processed with this admission profile.

FILE-NAME =
Determines which files or library members under your user ID may be accessed by FT requests that use this admission profile.

FILE-NAME = *NOT-RESTRICTED
Permits unrestricted access to all files and library members of the user ID.

FILE-NAME = <filename 1..54> / <c-string 1..512 with-low> /
***POSIX(NAME = <posix-pathname 1..510>)**
Only the specified file may be accessed. However, openFT is also able to generate unique filenames automatically, thus providing an easy way of avoiding conflicts. This is done by specifying the string %UNIQUE at the end of the filename which is predefined here (see section "File names" in the User Guide). When follow-up processing is specified, this file can be referenced with %FILENAME.
You can also directly specify file transfer with file pre- or post-processing here by entering a pipe symbol '|' followed by a command.

FILE-NAME = *EXPANSION(PREFIX = <filename 1..53> / <partial-filename 2..53> / <c-string 1..511 with-low>)

Restricts access to a number of files which all begin with the same prefix. If a *filename* is entered in an FT request which works with this admission profile, FTAC sets the *prefix* defined with EXPANSION in front of this filename. The FT request is then permitted to access the file *PrefixFilename*.

Example

– PREFIX=JACK.; an FT request in which FILE-NAME=BOERSE is specified, then accesses the file JACK.BOERSE.

Please note that the part of a DVS filename which is specified in the file transfer command still has to be of the type <filename>.

If you want to perform file transfer with pre- or post-processing, you should indicate this by entering the pipe symbol ‘|’ at the start of the prefix. The created FTAC profile can then be used only for file transfer with pre- or post-processing since the file name that is generated also starts with a ‘|’. The variable %TEMPFILE can also be used in the filename prefix. You can find detailed information on preprocessing and postprocessing in the section of the same name in the User Guide.

The maximum length of the entire pre- or post-processing command is limited to the maximum length of the file name. If several commands are specified, then they must be separated by a semicolon (‘;’).
There must not be a space between the semicolon and the slash.

Example

```
FILE-NAME = C‘|/Command1;/Command2;/Command3; ...‘
```

If you specify a name prefix that starts with a pipe character with *EXP(PREFIX=...), the preprocessing or postprocessing command of the FT request must not contain any semicolons. If the preprocessing or postprocessing command nevertheless contains semicolons, it must be enclosed in '...' (single quotes) or "..." (double quotes).

Special cases

– A file name or file name prefix that begins with the string '|ftexecsv' must be specified for admission profiles that are to be exclusively used for the ftexec command (see “Example 3” on page 177).

– Specify the file name prefix '|*ftmonitor' for admission profiles that are exclusively used for monitoring. A profile of this sort can then be used in the openFT Monitor or in an ft or ncopy command from a Windows or Unix system (see “Example 2” on page 177).

FILE-NAME = *LIBRARY-ELEMENT(...)

Determines which of your libraries and library members may be accessed by FT requests which use this admission profile.

LIBRARY =
Defines which libraries may be accessed with this admission profile.

LIBRARY = *NOT-RESTRICTED
The admission profile does not restrict access to libraries.

LIBRARY = <filename 1..54>
Only this library may be accessed.

LIBRARY = *EXPANSION(PREFIX = <filename 1..53> / <partial-filename 2..53>)
Only those libraries may be accessed which begin with the specified prefix. FTAC sets the prefix in front of a library name in an FT request which works with this admission profile, and then permits access to the library *Prefix-Libraryname*.

ELEMENT =
Determines which library members may be accessed with this admission profile.

ELEMENT = *NOT-RESTRICTED
Permits unrestricted access to library members.

ELEMENT = <composed-name 1..64 with-under>(...)
Permits access to the specified library member.

VERSION =
Access is only permitted for a specific version of the library member.

VERSION = *STD
Permits access only to the highest version of the library member.

VERSION = <text 1..24>
Access is only permitted for this version of the library member.

ELEMENT = *EXPANSION(PREFIX = <partial-filename 2..63> / <composed-name 1..63 with-under)
Defines a prefix. When a name for a library member is specified in an FT request which works with this admission profile, FTAC adds the specified prefix to this member name. The admission profile then permits access to this member with the name *PrefixMembername*.

TYPE =
Specifies a certain type of library member. The admission profile then only permits access to library members of this type.

TYPE = *NOT-RESTRICTED
Access is not restricted to a certain type of library member.

TYPE = <name 1..8>
FT requests which work with this admission profile may only access library members of this type.

FILE-PASSWORD =
You can enter a password for files into the admission profile. The FTAC functionality then only permits access to files which are protected with this password and to unprotected files. When a FILE-PASSWORD is specified in an admission profile, the password may no longer be specified in an FT request which uses this admission profile. This allows you to permit access to certain files to users in remote systems, without having to give away the file passwords.

FILE-PASSWORD = *NOT-RESTRICTED
Permits access to all files. If a password is set for a file, then it must be specified in the transfer request.

FILE-PASSWORD = *NONE
Only permits access to files without file passwords.

**FILE-PASSWORD = <c-string 1..4> / <x-string 1..8> /
<integer -2147483648..2147483647>**
Only permits access to files which are protected with the password specified and to unprotected files. The password which has already been specified in the profile may not be repeated in the transfer request. PASSWORD=*NONE would be entered in this case!

FILE-PASSWORD = *SECRET
The system prompts you to enter the password. However, the password does not appear on the screen.

PROCESSING-ADMISSION =
You can enter a user ID in your BS2000 system . Any follow-up processing of an FT request will be executed under this user ID. With PROCESSING-ADMISSION in the admission profile, you do not need to disclose your LOGON authorization to partner systems for follow-up processing.

PROCESSING-ADMISSION = *SAME
For the PROCESSING-ADMISSION, the values of the USER-ADMISSION are used. If *SAME is entered here, then any FT request which uses this profile must also contain PROCESSING-ADMISSION=*SAME or PROCESSING-ADMISSION=*NOT-SPECIFIED.

PROCESSING-ADMISSION = *NOT-RESTRICTED
FT requests which use this admission profile may contain any PROCESSING-ADMISSION. If you wish to perform follow-up processing with FTAM partners, PROCESSING-ADMISSION must have a value other than *NOT-RESTRICTED.

PROCESSING-ADMISSION = *PARAMETERS(...)
You can also enter the individual components of the user ID. This allows you to keep FT requests which use this admission profile under a different account number, for example. Or, a password can be set in the admission profile. FT requests which use this admission profile will then only function if their current LOGON password corresponds to the pre-set password.

USER-IDENTIFICATION =
Identifies the user ID under which the follow-up processing is to be executed.

USER-IDENTIFICATION = *SAME
The USER-IDENTIFICATION is taken from the USER-ADMISSION.

USER-IDENTIFICATION = *NOT-RESTRICTED
The admission profile does not restrict the user ID for the follow-up processing.

USER-IDENTIFICATION = <name 1..8>
FT requests which are processed with this admission profile are only permitted follow-up processing under this user ID. If another user ID is entered here, the parameter PASSWORD must also be entered. PASSWORD=*SAME is then not valid.

ACCOUNT =
Account number for the follow-up processing.

ACCOUNT = *SAME
The account number is taken from the USER-ADMISSION.

ACCOUNT = *NOT-RESTRICTED
Account number in FT requests which work with the admission profile. The admission profile does not restrict the account with regard to follow-up processing.

ACCOUNT = *NONE
The account number is used which is defined as the default account number of the user ID specified in the USER-IDENTIFICATION at the time the admision profile is used.

ACCOUNT = <alphanum-name 1..8>
Follow-up processing is to be settled under this account number.

PASSWORD =
You specify, where applicable, the BS2000 passwordfor the user ID specified in the USER-IDENTIFICATION under which the follow-up processing is to be executed. Here, you can enter a PASSWORD when the user ID in question doesn’t have such a password (yet).

PASSWORD = *SAME
The value *SAME is only valid if the PROCESSING-ADMISSION refers to your own user ID. If PASSWORD=*OWN is entered on USER-ADMISSION, then the password valid at the time of the request is used for the PROCESSING-ADMISSION.
The entry *SAME is only possible here if the follow-up processing is not started with the /ENTER command.

PASSWORD = *NOT-RESTRICTED
Specifies the password in FT requests which work with the admission profile. The admission profile does not restrict the password with regard to follow-up processing.

PASSWORD = *NONE
FT requests which use this admission profile can only initiate follow-up processing on user IDs without a password.

PASSWORD = <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
FT requests which use this admission profile may only initiate follow-up processing on user IDs which are protected with this password.

PASSWORD = *SECRET
The system prompts you to enter the password. The entry does not appear on the screen.

SUCCESS-PROCESSING =
Restricts the follow-up processing which an FT request is permitted to initiate in your system after a successful data transfer.

SUCCESS-PROCESSING = <u>*NOT-RESTRICTED</u>
In FT requests which use this admission profile the operand SUCCESS-PROCESSING may be used without restriction.

SUCCESS-PROCESSING = *NONE
The admission profile does not permit follow-up processing after successful data transfer.

SUCCESS-PROCESSING = <c-string 1..1000 with-low>
Commands which are executed in the local system after successful data transfer.
Individual commands must be preceded by a slash (/).
The individual commands must be separated by a semicolon (;). If a character string is enclosed by single or double quotes (’ or ”) within a command sequence, openFT does not interpret any semicolons within this character string as a separator.

SUCCESS-PROCESSING = *EXPANSION(...)
If a SUCCESS-PROCESSING was specified in an FT request which uses this admission profile, FTAC adds the prefix or suffix specified here to this command. As follow-up processing, the command which has been thus expanded is then executed.

If a suffix or prefix is defined at this point, then no command sequence for the follow-up processing may be specified in FT requests which use this admission profile. This makes the setting of prefixes and suffixes mandatory.

PREFIX = <u>*NOT-RESTRICTED</u>
Follow-up processing is not restricted by a prefix.

PREFIX = <c-string 1..999 with-low>
The specified prefix is set in front of a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the prefix is executed as follow-up processing.

SUFFIX = <u>*NOT-RESTRICTED</u>
The follow-up processing is not restricted by a suffix.

SUFFIX = <c-string 1..999 with-low>
The specified suffix is added to a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the suffix is executed as follow-up processing.

Example

If PREFIX=’/PRINT-FILE ’ is defined and SUCC=’filename’ specified in the FT request, then FT executes the command “/PRINT-FILE filename” as follow-up processing.

FAILURE-PROCESSING =
Restricts the follow-up processing which an FT request is permitted to initiate in your system after a failed data transfer.

FAILURE-PROCESSING = *NOT-RESTRICTED
In FT requests which use this admission profile the operand FAILURE-PROCESSING may be used without restriction.

FAILURE-PROCESSING = *NONE
The admission profile does not permit follow-up processing after failed data transfer.

FAILURE-PROCESSING = <c-string 1..1000 with-low>
Commands which are executed in the local system after failed data transfer.
Individual commands must be preceded by a slash (/).
The individual commands must be separated by a semicolon (;). If a character string is enclosed by single or double quotes (’ or ”) within a command sequence, openFT does not interpret any semicolons within this character string as a separator.

FAILURE-PROCESSING = *EXPANSION(...)
If a FAILURE-PROCESSING was specified in an FT request which uses this admission profile, FTAC adds the prefix or suffix specified here to this command. As follow-up processing, the command which has been thus expanded is then executed.

If a suffix or prefix is defined at this point, then no command sequence for the follow-up processing may be specified in FT requests which use this admission profile. This makes the setting of prefixes and suffixes mandatory.

PREFIX = *NOT-RESTRICTED
Follow-up processing is not restricted by a prefix.

PREFIX = <c-string 1..999 with-low>
The specified prefix is set in front of a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the prefix is executed as follow-up processing.

SUFFIX = *NOT-RESTRICTED
The follow-up processing is not restricted by a suffix.

SUFFIX = <c-string 1..999 with-low>
The specified suffix is added to a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the suffix is executed as follow-up processing.

WRITE-MODE =
Determines the WRITE-MODE specification which is valid for this FT request. WRITE-MODE is only effective if the receive file is in the same system as the admission profile definition.

WRITE-MODE = <u>*NOT-RESTRICTED</u>
In an FT request which accesses this admission profile, the operand WRITE-MODE may be used without restrictions.

WRITE-MODE = *NEW-FILE
In the FT request, *NEW-FILE, *REPLACE-FILE or *EXTEND-FILE may be entered for WRITE-MODE. If the receive file already exists, the transfer will be rejected.

WRITE-MODE = *REPLACE-FILE
In the FT request of openFT or FTAM partners, only *REPLACE-FILE or *EXTEND-FILE may be entered for WRITE-MODE. With ftp partners, *NEW-FILE may also be entered if the file does not yet exist.

WRITE-MODE = *EXTEND-FILE
In the FT request, only *REPLACE-FILE or *EXTEND-FILE may be entered for WRITE-MODE.

FT-FUNCTION =
Permits the restriction of the profile validity to certain FT functions (=file transfer and file management functions).

FT-FUNCTION = <u>*NOT-RESTRICTED</u>
The full scope of FT functions is available. For reasons of compatibility, the specification NOT-RESTRICTED means that FILE-PROCESSING REMOTE-ADMINISTRATION are not permitted! All other functions are permitted if this value is specified.

FT-FUNCTION = (*TRANSFER-FILE, *MODIFY-FILE-ATTRIBUTES, *READ-DIRECTORY,*FILE-PROCESSING, *REMOTE-ADMINISTRATION)
The following file transfer functions are available:

***TRANSFER-FILE**
The admission profile may be used for the file transfer functions “transfer files”, “view file attributes” and “delete files”.

***MODIFY-FILE-ATTRIBUTES**
The admission profile may be used for the file transfer functions “view file attributes” and “modify file attributes”.

***READ-DIRECTORY**
The admission profile may be used for the file transfer functions “view directories” and “view file attributes”.

***FILE-PROCESSING**
The admission profile may be used for the “pre-processing” and “post-processing” file transfer function. The “transfer files” function must also be permitted.

The *FILE-PROCESSING specification is of relevance only for FTAC profiles without a filename prefix. Otherwise the first character of the filename prefix determines whether only normal data transfer (no pipe symbol |) or only pre-processing and post-processing (pipe symbol |) are to be possible with this FTAC profile.

***REMOTE-ADMINISTRATION**
The admission profile is allowed to be used for the "remote administration" function. This allows a remote administrator to administer the openFT instance using this profile. *REMOTE-ADMINISTRATION may only be specified by the FT administrator or FTAC administrator.

USER-INFORMATION =
Here, you enter a text in the admission profile. This text is displayed with the command SHOW-FT-PROFILE.

USER-INFORMATION = <ins>*NONE</ins>
No text is stored in the profile.

USER-INFORMATION = <c-string 1..100 with-low>
Here, you enter a character string containing user information.

DATA-ENCRYPTION =
Restricts the encryption option for user data.

DATA-ENCRYPTION = <ins>*NOT-RESTRICTED</ins>
The encryption option for user data is not restricted. Both encrypted and unencrypted file transfers are accepted.

DATA-ENCRYPTION = *NO
Only those file transfers which do not have encrypted user data are accepted, i.e. encrypted requests are rejected.
If the request is made in a BS2000 or z/OS, for example, it must be specified there in the NCOPY request DATA-ENCRYPTION=*NO.

DATA-ENCRYPTION = *YES
Only those file transfer requests that have encrypted user data are accepted, i.e. unencrypted requests are rejected.
If the request is made in a BS2000 or z/OS, for example, it must be specified there in the NCOPY request DATA-ENCRYPTION=*YES.

i When using restrictions for FILE-NAME, SUCCESS-PROCESSING and FAILURE-PROCESSING, keep in mind that

– a restriction for follow-up processing must always be made for SUCCESS- and FAILURE-PROCESSING. Otherwise, it is possible that users will avoid this step.

– PREFIX of FILE-NAME, SUCCESS-PROCESSING and FAILURE-PROCESSING must correspond,
e.g. FILE-NAME = *EXP(XYZ.),SUCC = *EXP('/PRINT-FILE XYZ.')

Example 1

Jack John wishes to create an admission profile for the following purpose:

Dylan Dack, employee at the Dack Goldmine, has his own BS2000 computer. He has to transfer monthly reports on a regular basis to his boss Jack‘s computer, JACKJOHN, using File Transfer. The file needs to have the name MONTHLYREPORT.GOLDMINE and is to be printed out after transfer.

Since Jack's admission set does not permit any “inbound” requests, he needs to give the profile privileged status (he/she is permitted to do this, since he is an FTAC administrator). The Goldmine computer has the security level 50. The command required to create such an admission profile is as follows:

```
/CREATE-FT-PROFILE NAME=GOLDMORE,                                      -
/                    TRANSFER-ADMISSION='monthlyreportfortheboss',  -
/                    PRIVILEGED=*YES,                                  -
/                    IGNORE-MAX-LEVELS=(INBOUND-RECEIVE=*YES,          -
/                    INBOUND-PROCESSING=*YES),                         -
/                    TRANSFER-DIRECTION=*FROM-PARTNER,                 -
/                    PARTNER=GOLDMINE,                                 -
/                    FILE-NAME=MONTHLYREPORT.GOLDMINE,                 -
/                    SUCCESS-PROCESSING=                               -
/                    '/PRINT-FILE␣MONTHLYREPORT.GOLDMINE',             -
/                    FAILURE-PROCESSING=*NONE,                         -
/                    WRITE-MODE=*REPLACE-FILE
```

The short form of this command is:

```
/CRE-FT-PROF␣GOLDMORE,TRANS-AD='monthlyreportfortheboss',              -
/PRIV=*YES,IGN-MAX-LEV=(I-R=*YES,I-P=*YES),TRANS-DIR=*FROM,            -
/PART=GOLDMINE, FILE-NAME=MONTHLYREPORT.GOLDMINE,                      -
/SUCC='/PRINT-FILE␣MONTHLYREPORT.GOLDMINE',FAIL=*NONE,                 -
/WRITE=*REPL
```

File management can also be performed with this admission profile (see the specifications for the IGNORE-MAX-LEVELS operand).

Dylan Dack, who keeps the monthly report for the goldmine in his BS2000 computer in the file NOTHINGBUTLIES, can use the following openFT command to send it to the central computer JACKJOHN and print it out there:

```
/TRANSFER-FILE˽TO,JACKJOHN,(NOTHINGBUTLIES),
               (FILE=*NOT-SPECIFIED,TRANS-AD='monthlyreportfortheboss')
```

Example 2

A profile is to be created that only allows monitoring.

```
CREATE-FT-PROFILE MONITOR,,'ONLYFTMONITOR'  -
   ,FILE-NAME=*EXP('|*FTMONITOR ') -
   ,FT-FUN=(*TRANS-F,*FILE-PROC)
```

The openFT Monitor can be started from a Unix or Windows system using this profile with the following command:

```
ftmonitor "-po=10" FTBS2 ONLYFTMONITOR
```

Alternatively, the monitoring values can be output as rows to a file (in this case ftbs2_data), for instance with the following command:

```
ncopy FTBS2!"-po=10" ftbs2_data ONLYFTMONITOR
```

Example 3

If you only want to use FTAC profiles for the ftexec command then you must specify a filename prefix that starts with the character string ’|ftexecsv’.

If a command or command prefix is also to be defined, you must specify it in the following form:

```
FILE-NAME=*EXP('|ftexecsv -p=command-prefix')
```

If the command string or the command prefix set in the profile for calling ftexec contains spaces, it must be enclosed in double quotes ("). Any double quotes in the command string must be entered twice.

If the entire command string is specified as a file name in the profile for ftexec, you can only specify a space (' ') as the command name when calling ftexec. The FTAC profile does not prevent a caller of ftexec from specifying further command parameters.

Example 4

You want to create a profile which can be used to run precisely one file processing command. A number of logging records are output in the example below.

```
/CR-FT-PRO NUR1VORV,,'GetLoggingRecords'              -
,FILE-NAME=*EXP('|ftexecsv -p="/SH-FT-LOG-REC ,"')  -
,FT-FUN=(*TRANS-F,*FILE-PROC)
```

The following command, for example, can be used to access the profile from a remote system:

– Unix system or Windows system:

```
ftexec FTBS2 3 GetLoggingRecords
```

– BS2000 system:

```
/EXE-REM-CMD FTBS2,'3','GetLoggingRecords'
```

– z/OS system:

```
FTEXEC FTBS2,'3','GetLoggingRecords'
```

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	FTC0051	A user ID with the same name already exists.
0	0	FTC0056	Transfer admission is blocked.
0	64	FTC0100	An FT profile with the same name already exists.
0	64	FTC0101	An FT profile with the specified transfer admission. already exists.
0	64	FTC0150	The access password is missing.
0	64	FTC0153	The owner identification entered is not the own user ID.
0	64	FTC0157	No authorization to create the profile. An FTAC administrator can only set up a profile with specification of the transfer admission if they know the complete user ID.
0	64	FTC0172	The User-Admission entered does not exist in the system.
0	64	FTC0173	The Processing-Admission entered does not exist in the system.
0	64	FTC0178	The partner name entered occurs several times.
0	64	FTC0182	Maximum length for partner names has been exceeded.
0	64	FTC0200	The total length of the two follow-up processing commands is too long.
0	64	FTC0255	A system error has occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.12 DELETE-FT-INSTANCE
Delete the administration entry of an openFT instance

Note on usage

User group: FT administrator

Functional description

This command deletes the administration entry of the instance. All of the variable data such as, for example, the request file are kept and can be re-activated with the same instance name by re-executing the CREATE-FT-INSTANCE command.

In the event that a user task has altered the deleted instance, this will only be recognized on the next attempt by openFT to access this instance. openFT commands for this instance are rejected in this case, issuing the message FTR1025. The user must set another instance using the SET-FT-INSTANCE command.

Format

DELETE-**FT**-**INST**ANCE
NAME = <alphanum-name 1..8>

Operands

NAME = <alphanum-name 1..8>
The name of the openFT instance that is to be deleted. The default instance cannot be deleted.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
24	64	FTR1024	Standard instance must not be deleted.
25	64	FTR1025	Instance does not exist.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.13 DELETE-FT-KEY-SET Delete a key pair set

Note on usage

User group: FT administrator

Alias name: FTDELKEY

Functional description

Using the DELETE-KEY-SET / FTDELKEY command, you are deleting the key pair set of a reference. The key pair consists of a private key, which is internally administered by openFT, and a public key.

Public keys are stored on the configuration user ID of the of the openFT instance (default: $SYSFJAM) under the name:

SYSPKF.R<key reference>.L<key length>

The key reference is a numeric designator for the version of the key pair. For each reference there are three keys with lengths of 768, 1024 and 2048 bits respectively.

A key pair set should only be deleted if no partner system uses the corresponding public key any longer. This means that, after creating a new key pair set using CREATE-FT-KEY-SET, the new public key should be made available to all of the partner systems in which the local system is to be authenticated.

There should always be at least one key pair set in your openFT instance, otherwise all requests will be carried out in unencrypted form.

Format

DELETE**-FT-KEY**-SET / **FTDELKEY**
REFERENCE = <integer 1..9999999>

Operands

REFERENCE = <integer 1..9999999>
Allows selection of the key pair set to be deleted. You will find the reference in the name of the public key file (see above).

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
2	0	FTR1030	Warning: last key pair deleted.
32	64	FTR1032	Last key pair must not be deleted.
35	64	FTR1035	Command only permissible for FT administrator.
37	64	FTR1037	Key reference unknown.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

Delete the key pair set with the public keys $SYSFJAM.SYSPKF.R137.L768, $SYSFJAM.SYSPKF.R137.L1024 and $SYSFJAM.SYSPKF.R137.L2048:

```
/DELETE-FT-KEY-SET REF=137
```

5.14 DELETE-FT-LOGGING-RECORDS Delete log records or offline log files

Note on usage

User group: FT administrator, FTAC administrator

Alias name: FTDELLOG

Functional description

With DELETE-FT-LOGGING-RECORDS you can, as FT or FTAC administrator, delete log records for all login names and all record types (FT, FTAC, ADM) from the current log file.

You can also delete offline log files which are no longer required. Offline log files can only be deleted in their entirety. It is not possible to delete individual log records from an offline log file.

In principle, openFT can write any number of logging records (until the disk is full). The FT administrator should save the existing logging records (e.g. to tape or as a file in CSV format) and at regular intervals (weekly, for example, if there is a large number of requests) and delete older logging records. This means, firstly, that logging records are retained for a long period, thereby ensuring continuous documentation, and secondly, that memory space is not occupied unnecessarily.

You save the log records, for example, by redirecting the output of SHOW-FT-LOGGING-RECORDS (Displaying logging records, page 315ff) to a file in CSV format (for more information, see SHOW-FT-LOGGING-RECORDS):

```
/ASSIGN-SYSLST LOGGING FILE
/SHOW-FT-LOGGING-RECORDS...,NUMBER=*ALL,OUTPUT=*SYSLST(*CSV)
```

When backing up logging records, CSV format should be preferred to the default format since in this format all the information is backed up “in a single line” and a variety of tools can be used for the further processing of the information.

When deleting logging records, the disk storage occupied by the log file is not released. The free space within the file is, however, used to store new records.

In the case of very large log files it may take several minutes to delete log records. To prevent inconsistencies, it is not possible to use the K2 key to interrupt the command.

In this case the following procedure is recommended:

► Switch the log file using MODIFY-FT-OPTIONS LOGGING=*CHANGE-FILES. The current log file is switched "offline". New log records are now written to a new log file.

► After a certain time, evaluate all log files in the offline log file and archive them using SHOW-FT-LOGGING-RECORDS.

► Delete the offline log file using DELETE-FT-LOGGING-RECORDS.

The default setting for the command DELETE-FT-LOGGING-RECORDS has changed in openFTV11.0. If you specify the command without parameters, the default value *PARAMETERS() is used instead of *ALL as previously, i.e. all log records are deleted that have been written up to 00:00 h of the current day. This means that the command remains downward compatible in terms of its behavior.

Format

```
DELETE-FT-LOGGING-RECORDS / FTDELLOG

SELECT = *ALL / *OWN / *PARAMETERS(...) / *LOGGING-FILES (...)

   *PARAMETERS(...)
   |   OWNER-IDENTIFICATION = *ALL / *OWN / <name 1..8>
   |  ,LOGGING-DATE = *TODAY / *TOMORROW / <date 8..10>
   |  ,LOGGING-TIME = 00:00 / <time 1..8>
   |  ,RECORD-TYPE = *ALL / *PARAMETERS(...)
   |      *PARAMETERS(...)
   |      |   FT = *ALL / *NONE
   |      |  ,FTAC = *ALL / *NONE
   |      |  ,ADM = *ALL / *NONE
   |  ,LOGGING-ID = *ALL / <alphanum-name 1..12>

   *LOGGING-FILES(...)
   |  BEFORE = *TIME(...)
   |      *TIME = (...)
   |      |  DATE = <date 8..10>
   |      |  ,TIME = 00:00 / <time1..8>
```

Operands

SELECT =
Selects a group of logging records.

SELECT = *ALL
Deletes all logging records.

SELECT = *OWN
Deletes all logging records of your own ID.

SELECT = *PARAMETERS(...)

OWNER-IDENTIFICATION =
User ID whose logging records are to be deleted.

OWNER-IDENTIFICATION = *ALL
The user ID is not a selection criterion.

OWNER-IDENTIFICATION = *OWN
Logging records in the user ID are deleted.

OWNER-IDENTIFICATION = <name 1..8>
User ID whose logging records are to be deleted.

LOGGING-DATE =
Date before which the logging records are to be deleted.

LOGGING-DATE = *TODAY
If a time was specified explicitly with LOGGING-TIME, all log records that were written before this time are deleted. If no date was specified, openFT deletes all log records that were written up to midnight inclusive of the previous day.

LOGGING-DATE = *TOMORROW
All logging records that were created before the command was input are deleted.

LOGGING-DATE = <date 8..10>
Date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2011-12-24 or 11-12-24 for the 24th of December, 2011. openFT then deletes only those logging records that were written before the date and time specified with LOGGING-TIME and LOGGING-DATE.

LOGGING-TIME =
Logging records written up to the specified time are deleted.

LOGGING-TIME = 00:00
If a date was specified explicitly with LOGGING-DATE, openFT deletes all log records written before the specified date. If no date was specified, openFT deletes all log records that were written up to midnight inclusive of the previous day.

LOGGING-TIME = <time 1..8>
Time for the day specified with LOGGING-DATE. openFT deletes all log records written before this time. You specify the time in the format *hh:mm:ss*, e.g. 14:30:10.

RECORD-TYPE =
Defines the type of logging records to be deleted.

RECORD-TYPE = *ALL
The record type is not a selection criterion.

RECORD-TYPE = *PARAMETERS(...)
Type of the logging record.

FT = *ALL / *NONE
Specifies whether or not the FT logging records are to be deleted.

FTAC = *ALL / *NONE
Specifies whether or not FTAC logging records are to be deleted.

Please note that the FTAC logging records can only be deleted by the FTAC administrator.

ADM = *ALL / *NONE
Specifies whether ADM log records are deleted or not.

LOGGING-ID =
Selects the logging records on the basis of the logging ID.

LOGGING-ID = *ALL
The logging ID is not a selection criterion.

LOGGING-ID = <alphanum-name 1..12>
All logging records with a logging ID smaller than or equal to the specified value are deleted.

SELECT = *LOGGING-FILES(...)
Controls the deletion of offline log files. Offline log records cannot be deleted individually: only entire files can be deleted.

BEFORE = *TIME(...)
Deletes all the offline log files which were switched offline on or before the specified time (local time!) by switching the log file offline. This ensures that only log records which are at least as old as the specified time are deleted.

If you enter the current date or a date in the future, then all the existing offline log files are deleted.

DATE = <date 8..10>
Creation date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2012-03-31 or 12-03-31 for March 31, 2012.

TIME = 00:00 / <time 1..8>
Time for the date specified with DATE. You enter the time in the format *hh:mm:ss*, e.g. 14:30:10.

i Up to 1024 log files can be deleted per call. If you wish to delete more files, repeat the call.

Under some circumstances it may not be possible to immediately delete a log file which has just been switched to become an offline log file after it has been switched if the file still has synchronous requests open.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	No log records available for the selection criteria.
83	32	CMD0221	Internal error.
34	64	FTR1034	Command only permissible for FT or FTAC administrator.
35	64	FTR1035	Command only permissible for FT administrator.
36	64	FTR1036	User not authorized for other user Ids

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section "Command return codes" on page 133

Example

The FT administrator wishes to delete all FT log records from the current log file, but not FTAC and ADM log records (if these are present):

```
/DELETE-FT-LOGGING-RECORDS  SELECT=*PARAMETERS(LOGGING-DATE=*TOMORROW, -
/                       RECORD-TYPE=*PARAMETERS(FTAC=*NONE,ADM=*NONE))
```

5.15 DELETE-FT-PROFILE Delete admission profile

Note on usage

User group: FTAC user and FTAC administrator

A prerequisite for using this command is the use of openFT-AC.

Functional description

With the command DELETE-FT-PROFILE , you can delete all admission profiles of which you are the owner. In your role as FTAC administrator, you can also delete the admission profiled of any users. You should occasionally thin out the set of profiles to ensure that there are no out-of-date admission profiles in your system that could potentially threaten the security of your system.

With SHOW-FT-PROFILE (see page 372ff), you can view the profiles and decide which ones you no longer need.

Format

```
DELETE-FT-PROFILE

 NAME = *ALL / <alphanum-name 1..8> / *STD
,PASSWORD = *NONE / <c-string 1..8 with-low> / <x-string 1..16> / *SECRET
,SELECT-PARAMETER = *OWN / *PARAMETERS(...)

   *PARAMETERS(...)
     |  TRANSFER-ADMISSION = *ALL / *NOT-SPECIFIED / <alphanum-name 8..32> /
     |                                <c-string 8..32 with-low> / <x-string 15..64> / *SECRET
     | ,OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
```

Operands

NAME =
You can access the admission profile to be deleted using its name.

NAME = *ALL
Deletes all admission profiles. The FTAC user can delete all of his/her admission profiles with this operand if he/she does not select a special profile with SELECT-PARAMETER. The administrator can delete his/her own profiles with this entry. He/She can also use SELECT-PARAMETER to delete all the admission profiles of a particular user or all the admission profiles in the system.

NAME = <alphanum-name 1..8>
Deletes the admission profile with the specified name.

NAME = *STD
Deletes the default admission profile for your own user ID.

PASSWORD =
You enter the FTAC password which permits you to use FTAC commands with your user ID.

PASSWORD = *NONE
No FTAC password is required.

PASSWORD = <c-string 1..8 with-low> / <x-string 1..16>
Specifies the corresponding FTAC password.
If the FTAC administrator has defined an FTAC password, then this password must be entered here if he/she wishes to delete the profiles of other users.

PASSWORD = *SECRET
The system prompts you to enter the password. However, the password does not appear on the screen.

SELECT-PARAMETER =
You can enter selection criteria for the admission profiles to be deleted.
FTAC users can address the admission profiles to be deleted using their TRANSFER ADMSSION.
FTAC administrators can address the admission profiles to be deleted using their TRANSFER ADMISSION or OWNER IDENTIFICATION.

SELECT-PARAMETER = *OWN
Deletes your own admission profiles.

SELECT-PARAMETER = *PARAMETERS(...)
With this structure, you can enter individual selection criteria.

TRANSFER-ADMISSION =
You can use the transfer admission of an admission profile as a selection criterion for deletion.

TRANSFER-ADMISSION = *ALL
Deletes admission profiles irrespective of the TRANSFER-ADMISSION.

TRANSFER-ADMISSION = *NOT-SPECIFIED
Deletes admission profiles for which no transfer admission is specified.

TRANSFER-ADMISSION = <alphanum-name 8..32> / <c-string 8..32 with-low> / <x-string 15..64>
Deletes the admission profile which is accessed with this transfer admission. The alphanumeric entry is always saved in lower-case letters. The FTAC user can only enter the transfer admissions of his/her own admission profiles.

TRANSFER-ADMISSION = *SECRET
The system prompts you to enter the transfer admission. This does not appear on the screen.

OWNER-IDENTIFICATION =
Deletes a specific owner's admission profile. The FTAC user can only delete his/her own profiles. The FTAC administrator can also enter foreign user IDs.

OWNER-IDENTIFICATION = *OWN
Deletes your own admission profile.

OWNER-IDENTIFICATION = *ALL
Allows the FTAC administrator to delete admission profiles of all user IDs. The FTAC user is not permitted to use this entry.

OWNER-IDENTIFICATION = <alphanum-name 1..8>
The FTAC user can only specify his/her own user ID; the effect corresponds to *OWN. The FTAC administrator deletes the admission profiles under this user ID.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	64	FTC0053	No FT profile exists with these criteria.
0	64	FTC0150	The access password is missing.
0	64	FTC0153	The owner identification entered is not the user's own ID.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section "Command return codes" on page 133

5.16 EXECUTE-REMOTE-FTADM-CMD Execute remote administration command

Note on usage

User group: Users configured as remote administrators on the remote administration server.

A remote administration server must be deployed in order to use this command.

Description of the function

The EXECUTE-REMOTE-FTADM-CMD command allows you to act as a remote administrator and administer an openFT instance via a remote administration server. The remote administration server accepts the administration request, checks the authorization and forwards the request to the openFT instance that is to be administered.

In addition, as remote administrator, you can use EXECUTE-REMOTE-FTADM-CMD command to query the following information from the remote administration server (see page 198):

- You can determine what openFT instances you are authorized to administer and what remote administration permissions you have for these instances.
- You can read the ADM traps that the openFT instances you are administering have sent to the remote administration server. For this to be possible, the remote administration server must also be configured as an ADM trap server for the administered openFT instances. For details, see the section “ADM traps” on page 106.

Format

```
EXECUTE-REMOTE-FTADM-CMD / FTADM

 PARTNER-SERVER = <text 1..200 with-low>
,TRANSFER-ADMISSION = <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...)
,ROUTING-INFO = <text 1..200 with-low> / <c-string 1..200 with-low> / *NONE
,CMD = <c-string 1..1800 with-low>
,OUTPUT = *SYSOUT / *SYSLST  / *FILE(...)
    *FILE(...)
      |    FILE-NAME = <filename 1..54>
,DATA-ENCRYPTION = *NO / *YES
```

Operands

PARTNER-SERVER= <text 1..200 with-low>
Specifies the partner name in the partner list or the address of the remote administration server. The remote administration server must be addressed as an ADM partner. For details, see the section section “Defining partner properties” on page 44.

TRANSFER-ADMISSION =
Specifies the FTAC transfer admission for accessing the remote administration server.

ROUTING-INFO =
Contains the routing information required to forward the remote administration command from the remote administration server to the required openFT instance.

ROUTING-INFO = <text 1..200 with-low> / <c-string 1..200 with-low>
Specifies the pathname of the openFT instance that you want to administer. The pathname is configured on the remote administration server by the ADM administrator. You can get the pathname by running the command ftshwc on the remote administration server, see the section “Determining the names of the openFT instances” on page 104.

ROUTING-INFO = *NONE
No routing information is required, i.e. the command is executed directly on the remote administration server. Only specific commands, however, (ftshwc and ftshwatp) can be executed directly on the remote administration server. You will find a brief description of these commands on page 198.

CMD =
Remote administration server command in the syntax of the openFT instance to be administered. A remote administration command can only be processed if the remote system is using an FT product that supports this function (see the section “Remote administration commands” on page 193).

CMD = <c-string 1..1800 with-low>
The remote administration command to be executed.

OUTPUT =
Specifies where the data generated by the command should be output following transfer in the local system.
If the partner is a BS2000 system, output to SYSLST from the remote command is redirected to the channel specified here. Output to SYSOUT is always shown locally on SYSOUT.

OUTPUT = *SYSOUT
The data is written to *SYSOUT.

OUTPUT = *SYSLST
The data is written to *SYSLST.

OUTPUT = *FILE(...)
The data is written to a file. Please note that only the data which the command specified with CMD outputs to *SYSLST (BS2000) or *STDOUT (on z/OS) or stdout (on a Unix/Windows system) is written to file.

FILE**-NAME = <filename 1..54>**
Name of the output file.

DATA-ENCRYPTION =
Specifies whether the data is to be transferred in encrypted form. The encryption of the request description data is not affected by this parameter.

DATA-ENCRYPTION = *NO
The data is transferred unencrypted.

DATA-ENCRYPTION = *YES
The data is transferred encrypted.

Command return codes

(SC2)	SC1	Maincode	Meaning/Guaranteed messages
108	128	FTR0108	Request rejected. Remote system not accessible.
4	1	CMD0202	The selected parameters could not be specified simultaneously.
33	32	CMD0221	Request rejected. Internal error.
36	32	CMD0221	Request rejected. Inconsistent request data.
83	32	CMD0221	Internal error.
51	64	FTR2051	Encryption not possible for this request.
52	64	FTR2052	Request rejected by central remote administration server
54	64	FTR2054	Command invalid
125	128	FTR2125	Request rejected. Transport connection lost.
169	64	FTR2169	Request rejected. Remote system: Transfer admission invalid. Transfer admission incorrect or missing FTAC admissions.
170	64	FTR2170	Request rejected. Remote system: Function not supported.
rc	64	FTR2207	The command returned an error in the remote system. The exit code of the remote command can be queried using subcode 2 (rc).

SC1/2 = Subcode 1/2 in decimal notation
For additional information refer to the section “Command return codes” on page 133.

5.16.1 Remote administration commands

The following tables list the possible remote administration commands on the individual openFT platforms and on the remote administration server. The Permission column shows the permission required to execute the command as a remote administration command. The following permissions are possible:

FTOP	Read FT access (FT operator)
FT	Read and modify FT access (FT administrator)
FTAC	Read and modify FTAC access (FTAC administrator)

If a number of permissions are specified, e.g. FT | FTAC, it is sufficient if one of these permissions applies, i.e. FT or FTAC.

In the case of a remote administration request, these permissions are compared with the permissions you have on the relevant instance as a remote administrator. The ADM administrator defines the permissions in the configuration data of the remote administration server. If your permissions are not sufficient, the request is rejected and an appropriate message is issued.

Commands for openFT partners in BS2000

The commands have to be prefixed with "\" (backslash) before the command name.

BS2000 command	Short forms and aliases	Permission
ADD-FT-PARTNER	ADD-FT-PART FTADDPTN	FT
CANCEL-FILE-TRANSFER	CAN-FILE-T, CNFT NCANCEL, NCAN FTCANREQ	FT
CREATE-FT-KEY-SET	CRE-FT-KEY FTCREKEY	FT
CREATE-FT-PROFILE	CRE-FT-PROF	FTAC
DELETE-FT-KEY-SET	DEL-FT-KEY FTDELKEY	FT
DELETE-FT-LOGGING-RECORDS	DEL-FT-LOG-REC FTDELLOG	FT | FTAC
DELETE-FT-PROFILE	DEL-FT-PROF	FTAC
IMPORT-FT-KEY [1]	IMP-FT-KEY FTIMPKEY	FT
MODIFY-FILE-TRANSFER	MOD-FILE-T FTMODREQ	FT
MODIFY-FT-ADMISSION-SET	MOD-FT-ADM	FTAC
MODIFY-FT-KEY [1]	MOD-FT-KEY FTMODKEY	FT
MODIFY-FT-OPTIONS	MOD-FT-OPT FTMODOPT	FT
MODIFY-FT-PARTNER	MOD-FT-PART FTMODPTN	FT
MODIFY-FT-PROFILE	MOD-FT-PROF	FTAC
REMOVE-FT-PARTNER	REM-FT-PART FTREMPTN	FT
SHOW-FILE-TRANSFER	SHOW-FILE-T, SHFT NSTATUS, NSTAT FTSHWREQ	FT | FTOP
SHOW-FT-ADMISSION-SET	SHOW-FT-ADM-S	FTAC
SHOW-FT-DIAGNOSTIC	SHOW-FT-DIAG FTSHWD	FT | FTOP | FTAC
SHOW-FT-INSTANCE	SHOW-FT-INST	FT | FTOP

BS2000 command	**Short forms and aliases**	**Permission**
SHOW-FT-KEY [1]	FTSHWKEY	FT | FTOP
SHOW-FT-LOGGING-RECORDS	SHOW-FT-LOG-REC FTSHWLOG	FT | FTOP | FTAC
SHOW-FT-MONITOR-VALUES [2]	SHOW-FT-MON-VAL FTSHWMON	FT | FTOP
SHOW-FT-OPTIONS	SHOW-FT-OPT FTSHWOPT	FT | FTOP
SHOW-FT-PARTNERS	SHOW-FT-PART FTSHWPTN	FT | FTOP
SHOW-FT-PROFILE	SHOW-FT-PROF	FTAC
START-FTTRACE	FTTRACE	FT | FTOP
STOP-FT	FTSTOP	FT
UPDATE-FT-PUBLIC-KEYS	UPD-FT-PUB-KEY FTUPDKEY	FT

[1] As of V12.0

[2] As of V11.0

Commands for openFT partners in z/OS

z/OS command	Alias	Permission
FTADDPTN		FT
FTCANREQ	NCANCEL, NCAN	FT
FTCREKEY		FT
FTCREPRF		FTAC
FTDELKEY		FT
FTDELLOG		FT | FTAC
FTDELPRF		FTAC
FTHELP		FT | FTOP | FTAC
FTIMPKEY [1]		FT
FTINFO		FT | FTOP | FTAC
FTMODADS		FTAC
FTMODKEY [1]		FT
FTMODOPT		FT
FTMODPRF		FTAC
FTMODPTN		FT
FTMODREQ		FT
FTREMPTN		FT
FTSHWADS		FTAC
FTSHWD		FT | FTOP | FTAC
FTSHWINS		FT | FTOP
FTSHWKEY [1]		FT | FTOP
FTSHWLOG		FT | FTOP | FTAC
FTSHWMON [2]		FT | FTOP
FTSHWNET		FT | FTOP
FTSHWOPT		FT | FTOP
FTSHWPRF		FTAC
FTSHWPTN		FT | FTOP
FTSHWREQ	NSTATUS, NSTAT	FT | FTOP
FTSTOP		FT
FTTRACE		FT | FTOP
FTUPDKEY		FT

[1] As of V12.0

[2] As of V11.0

Commands for openFT partners in Unix and Windows systems

Command	Comment	Permission
fta	up to V10.0	FT
ftaddlic	Windows systems as of V12.0 only	FT
ftaddptn		FT
ftc	up to V10.0	FT
ftcanr		FT
ftcans	openFT-Script command	FT
ftcrek		FT
ftcrep		FTAC
ftdelk		FT
ftdell		FT | FTAC
ftdelp		FTAC
ftdels	openFT-Script command	FT
fthelp		FT | FTOP | FTAC
fti	up to V10.0	FT | FTOP
ftimpk	as of V12.0	FT
ftinfo		FT | FTOP | FTAC
ftmoda		FTAC
ftmodk	as of V12.0	FT
ftmodo		FT
ftmodp		FTAC
ftmodptn		FT
ftmodr		FT
ftremlic	Windows systems as of V12.0 only	FT
ftping		FT | FTOP
ftremptn		FT
ftrs	up to V10.0	FT
ftsetpwd	Windows systems only	FT | FTOP
ftshwa		FTAC
ftshwact	openFT-Script command	FT | FTOP
ftshwd		FT | FTOP | FTAC
ftshwi		FT | FTOP
ftshwk	as of V12.0	FT | FTOP

Command	**Comment**	**Permission**
ftshwl		FT I FTOP I FTAC
ftshwlic	Windows systems as of V12.0 only	FT
ftshwm	as of V11.0	FT I FTOP
ftshwo		FT I FTOP
ftshwp		FTAC
ftshwptn		FT I FTOP
ftshwr		FT I FTOP
ftshws	openFT-Script command	FT I FTOP
ftstop		FT
fttrace		FT I FTOP
ftupdk		FT

Commands on the remote administration server

EXECUTE-REMOTE-FTADM-CMD allows you to execute the commands *ftshwc* and *ftshwatp* on the remote administration server. To do this, you must specify ROUTING-INFO=*NONE:

Command	**Comment**	**Permission**
ftshwc	Gets the instances that the remote administrator is permitted to administer.	FT I FTOP I FTAC (I.e. all instances are displayed for which the remote administrator has this permission.)
ftshwatp	Outputs the ADM traps of the openFT instances that can be administered.	FT I FTOP (I.e. ADM traps of all instances are displayed for which the remote administrator has this permission.)

These commands also provide further options. For details, see, for instance, the manual "openFT V12.0 for Unix Systems - Installation and Administration".

5.17 EXPORT-FTAC-ENVIRONMENT
Export FTAC admission profiles and sets

Note on usage

User group: FTAC administrator

openFT-AC must be installed to use this command.

Functional description

The FTAC administrator can easily “move” admission profiles and sets when a user migrates from one computer to another. The commands EXPORT-FTAC-ENVIRONMENT and IMPORT-FTAC-ENVIRONMENT are intended for this purpose.

This commands are not available to FTAC users!

The commands only affect the currently set openFT instance. If necessary, the FTAC administrator must create them under several openFT instances.

Export files cannot be extended. They must be deleted and created again if necessary.

Format

```
EXPORT-FTAC-ENVIRONMENT

 TO-FILE = <filename 1..54>
,USER-IDENTIFICATION = *ALL / list-poss(100): <name 1..8>
,SELECT-PARAMETER = *ALL / *PARAMETERS(...)
   *PARAMETERS(...)
   |   PROFILE-NAME = *ALL / *NONE / list-poss(100): <alphanum-name 1..8>
   |  ,ADMISSION-SET = *YES / *NO
```

Operands

TO-FILE = <filename 1..54>
Name of the file in which the admission profiles and sets are output.

USER-IDENTIFICATION =
The user ID whose admission profiles and sets are to be output on file.

USER-IDENTIFICATION = *ALL
The admission profiles and sets of all user IDs are to be output on file.

USER-IDENTIFICATION = list-poss(100): <name 1..8>
The admission profiles and sets of the user IDs specified are to be output on file.

SELECT-PARAMETER =
Determines whether only admission profiles, only admission sets, or both are to be output on file. For admission profiles, you can select those which are to be output.

SELECT-PARAMETER = *ALL
All admission profiles and sets associated with the user ID specified under USER-IDENTIFICATION are to be output on file.

SELECT-PARAMETER = *PARAMETERS(...)
Specifies which of the admission profiles and sets associated with the USER-IDENTIFICATION are to be output on file.

PROFILE-NAME = *ALL
All admission profiles are output on file.

PROFILE-NAME = *NONE
No admission profiles are exported.

PROFILE-NAME = list-poss(100): <alphanum-name 1..8>
Only the profiles with the specified names (maximum 100) are output on file.

ADMISSION-SET = *YES
All admission sets are output on file.

ADMISSION-SET = *NO
No admission sets are exported.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	FTC0054	No information matches the specified criteria.
0	64	FTC0102	File already exists.
0	64	FTC0104	Access to the user ID denied or the user ID does not exist.
0	64	FTC0105	Access to the file denied.
0	64	FTC0106	Access to the temporary file denied.
0	64	FTC0156	The command may only be executed by the FTAC administrator.
0	64	FTC0180	The USER-ID entered occurs several times.
0	64	FTC0181	The FT profile name entered occurs several time.
0	64	FTC0206	Partially qualified file name too long.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.18 IMPORT-FTAC-ENVIRONMENT Import FTAC admission profiles and sets

Note on usage

User group: FTAC administrator

openFT-AC must be installed to use this command.

Functional description

The FTAC administrator can easily “move” admission profiles and sets when a user migrates from one computer to another. The commands EXPORT-FTAC-ENVIRONMENT and IMPORT-FTAC-ENVIRONMENT are intended for this purpose. These commands cannot be used by the FTAC user.
If the FTAC administrator does not possess TSOS privileges then all imported admission profiles will be locked.
This can be seen in the SHOW-FT-PROFILE command in the specification *LOCKED (by_import). Privileged profiles lose their privileged status when imported. They will also be designated as private.

These restrictions are not valid by default, if the FTAC administrator also has the TSOS privilege. In this case, profiles are imported unlocked and privileges are retained. If that is not desirable due to security concerns, the FTAC administrator can force locking by specifying the SECURITY=HIGH parameter.

An admissions profile is otherwise only imported if its name does not exist on the destination ID.

If the target computer already has an admission profile with the same transfer admission and the admission profile is designated as private, both transfer admissions are locked. The transfer admission of the old profile is set to *DUPLICATED and the transfer admission of the imported profile is set to *NOT-SPECIFIED. If the already existing admission profile is designated as ”public”, then it is not locked.

Format

IMPORT-**FTAC-ENV**IRONMENT

FROM-FILE = <filename 1..54>
,**USER-ID**ENTIFICATION = ***ALL** / list-poss(100): <name 1..8>
,**SEL**ECT-PARAMETER = ***ALL** / ***PAR**AMETERS(...)
    ***PAR**AMETERS(...)
        | **PROF**ILE-**NAME** = ***ALL** / ***NONE** / list-poss(100): <alphanum-name 1..8>
        | ,**AD**MISSION-**SET** = ***YES** / ***NO**
,**SECURITY** = ***STD** / ***HIGH**

Operands

FROM-FILE = <filename 1..54>
Name of the file from which the admission profiles and sets are to be imported. Temporary files may not be used. If the file contains invalid data or if there is an error while accessing the file, the command is rejected with the message FTC0103.

USER-IDENTIFICATION =
User ID whose admission profiles and sets are to be transferred from an export file.

USER-IDENTIFICATION = *ALL
The admission profiles and sets of all users are to be transferred.

USER-IDENTIFICATION = list-poss(100): <name 1..8>
The admission profiles and sets of the users specified (maximum 100) are to be transferred.

SELECT-PARAMETER =
Determines whether only admission profiles, only admission sets, or both are to be imported. For admission profiles, you can specify which are to be imported.

SELECT-PARAMETER = *ALL
All the admission profiles and sets associated with the user ID specified under USER-IDENTIFICATION are to be imported.

SELECT-PARAMETER = *PARAMETERS(...)
Specifies which of the admission profiles and sets associated with the USER-IDENTIFICATION are to be imported.

> **PROFILE-NAME = *ALL**
> All admission profiles are to be imported.
>
> **PROFILE-NAME = *NONE**
> No admission profiles are to be imported.

PROFILE-NAME = list-poss(100): <alphanum-name 1..8>
Only the profiles specified are to be imported (maximum 100).

ADMISSION-SET = *YES
All admission sets are to be imported.

ADMISSION-SET = *NO
No admission sets are to be imported.

SECURITY =
An FTAC administrator with TSOS privilege can use this operand to control security.

SECURITY = *STD
For FTAC administrators with TSOS privilege:
The profile attributes are not altered when imported.

For FTAC administrators not having the TSOS privilege:
This operand works like the specification *HIGH, i.e. the admissions profiles are locked (locked by import) and retain the attributes USAGE=PRIVATE and PRIVILEGED = NO.

SECURITY = *HIGH
The admissions profiles are locked (locked by import) and retain the attributes USAGE=PRIVATE and PRIVILEGED=NO.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	64	FTC0052	The information output was interrupted.
0	0	FTC0054	No information matches the specified criteria.
0	0	FTC0056	The transfer admission is locked.
0	64	FTC0100	An FT profile with the specified name already exists.
0	64	FTC0101	An FT profile with the specified transfer admission already exists.
0	64	FTC0103	The file is not an FTAC export file or access is denied.
0	64	FTC0104	Access to the user ID denied or the ID does not exist.
0	64	FTC0105	Access to the file denied.
0	64	FTC0106	Access to the temporary file denied.
0	64	FTC0156	The command can only be executed by the FTAC administrator.
0	64	FTC0177	The filename entered is unknown.
0	64	FTC0180	The USER-ID entered occurs several times.
0	64	FTC0181	The FT profile name entered occurs several times.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.19 IMPORT-FT-KEY Import key

Note on usage

User group: FT administrator

Alias name: FTIMPKEY

Functional description

You can use the IMPORT-FT-KEY command as FT administrator to import a partner’s public key or an RSA key pair.

Importing a public key

If you want to import the public key of a partner, the key must have been generated by the partner’s openFT instance and the partner must have been entered in the partner list. The key is then stored in the SYSKEY file under the name of the partner. Please ensure that the partner’s instance identification is entered correctly in the partner list.

Importing an RSA key pair

You can import an RSA key pair consisting of a public and a private key. The key pair can be used for data encryption and authentication like a key pair generated by openFT.

The key pair must be generated using an external tool. It must have the length 768, 1024 or 2048 bits and be present in PEM format (openSSL native PEM or PKCS#8) or in PKCS#12 V1.0 format.

If the key pair demands a password phrase (password), then this must be specified during the import.

During import, the same applies as for key pairs generated with CREATE-FT-KEY-SET:

- The key pair contains a unique reference number.
- The public key is stored under the name SYSPKF.R<key reference>.L<key length>

For details, see section “CREATE-FT-KEY-SET Create a key pair set” on page 155.

Format

```
IMPORT-FT-KEY / FTIMPKEY

PRIVATE-KEY = *NONE / *PARAMETERS(...)

    *PARAMETERS(...)
      | FILE-NAME = <filename 1..54>
      | ,PASSWORD = *NONE / *SECRET / <c-string 1..64 with-low>
      | ,TYPE = *PEM / *P12

,PUBLIC-KEY = *NONE / *PARAMETERS(...)

    *PARAMETERS(...)
      | FILE-NAME = <filename 1..54>
```

Operands

PRIVATE-KEY =
Specifies whether a private key is to be imported.

PRIVATE-KEY = *NONE
No private key is imported.

PRIVATE-KEY = *PARAMETERS(...)
Defines which private key is imported.

FILE-NAME = <filename 1..54>
Name of the file which contains the private key.

PASSWORD =
Password with which the private key is protected.

PASSWORD = *NONE
The private key is not protected by a password.

PASSWORD = *SECRET
You are requested by the system to enter the password. However, your entry is not displayed on the screen.

PASSWORD = <c-string 1..64 with-low>
Password with which the private key is protected.

TYPE =
Type of key file whose key is to be imported.

TYPE = *PEM
The key file is available in PEM format.

TYPE = *P12
The key file contains a certificate and a private key in accordance with the standard PKCS#12 V1.0. The file is searched for a private key and any non-supported elements (e.g. certificates, CRLs) are ignored during the import. The first private key that is found in the file is imported. Any others are ignored.
If the certificate is protected by a signature or hash, then openFT does not perform a validity check. The validity of the file must be verified using other means.

PUBLIC-KEY =
Specifies whether a public key is to be imported.

PUBLIC-KEY = *NONE
No public key is imported.

PUBLIC-KEY = *PARAMETERS(...)
Defines which public key is imported.

FILE-NAME = <filename 1..54>
Name of the file which contains the public key.

You must specify a file in at least one of the operands PRIVATE-KEY or PUBLIC-KEY.

Command return codes

(SC2)	SC1	Maincode	Bedeutung
0	0	CMD0001	Key pair has been imported
83	32	CMD0221	Internal error
29	64	FTR1029	Maximaum number of key pairs exceeded
35	64	FTR1035	Command only permissible for FT administrator
45	64	FTR1045	Partner name not found in partner list
69	64	FTR1065	Key file not found
66	128	FTR1066	Too little storage space for the file
69	64	FTR1069	Error while accessing the key file
83	64	FTR1083	Structure of the key file not supported
84	64	FTR1084	Invalid password
85	64	FTR1085	Password not specified
86	64	FTR1086	Key pair already exists

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.20 MODIFY-FILE-TRANSFER Modify request queue

Note on usage

User group: FT user and FT administrator

Alias name: FTMODREQ

Functional description

You use the MODIFY-FILE-TRANSFER command to modify the position and priority of your outbound requests within the openFT request queue. You have the option of processing the outbound requests in any order you wish. Newly input requests or requests whose priority changes are put at the end of the request queue for the corresponding priority. If already active requests are repositioned behind waiting outbound requests, the active requests are interrupted if possible in favor of those waiting.

MODIFY-FILE-TRANSFER is only valid for outbound requests.

The sequence of requests with a starting time in the future cannot be modified.

As FT administrator you can modify all requests.

Format

```
MODIFY-FILE-TRANSFER / FTMODREQ

 TRANSFER-ID = *ALL / <integer 1..2147483647>
,SELECT = *OWN / *PARAMETERS(...)

   *PARAMETERS(...)
        OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
       ,PARTNER = *ALL / <text 1..200 with-low>
       ,FILE = *ALL / <filename 1..54> / <c-string 1..512 with-low> /
                        *LIBRARY-ELEMENT(...)
          *LIBRARY-ELEMENT(...)
               LIBRARY = *ALL / <filename 1..54>
              ,ELEMENT = *ALL / <filename 1..64 without-gen-vers>(...) /
                                <composed-name 1..64 with-under>(...)
                 <filename>(...) / composed-name 1..64>(...)
                      VERSION = *ALL / <text 1..24>
              ,TYPE = *ALL / <name 1..8>
       ,MONJV = *NONE / <filename 1..54>
       ,JV-PASSWORD = *NONE / <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647> /
                              *SECRET

,QUEUE-POSITION = *UNCHANGED / *FIRST / *LAST

,PRIORITY = *UNCHANGED / *NORMAL / *HIGH / *LOW
```

Operands

TRANSFER-ID =
Transfer ID of the outbound request to be modified.

TRANSFER-ID = *ALL
Modifies all outbound requests, If further selections haven’t been specified with SELECT (see below).

TRANSFER-ID = <integer 1..2147483647>
Transfer ID which is communicated to the local system in the FT request confirmation.

SELECT =
Contains selection criteria for outbound requests to be modified. A request is only modified if all the criteria specified are met.

SELECT = *OWN
Modifies all FT requests of the user’s own ID.

SELECT = *PARAMETERS(...)

OWNER-IDENTIFICATION =
Identifies the owner of the FT request.

OWNER-IDENTIFICATION = <u>*OWN</u>
Modifies only outbound requests with the user's own ID.

OWNER-IDENTIFICATION = *ALL
Modifies outbound requests for all user IDs.
Only the FTAC administrator may use this entry.

OWNER-IDENTIFICATION = <name 1..8>
Specifies a user ID whose requests are to be modified.
Users may only enter their own user ID.

PARTNER =
Modifies outbound requests which are to be executed with a particular partner system.

PARTNER = <u>*ALL</u>
The name of the partner system is not selected as a criterion for the outbound requests to be modified.

PARTNER = <text 1..200 with-low>
Modifies outbound requests which are to be executed with this partner system. You can specify the name from the partner list or the address of the partner system. For more information on address specifications, see section "Defining partner properties" on page 44.

FILE =
Modifies outbound requests which access this file or library member in the local system as a send or receive file. The file or library member name must be entered exactly as in the file transfer request and as it is output using the SHOW-FILE-TRANSFER command. File names with wildcards are not permitted.

FILE = <u>*ALL</u>
The filename is not selected as a criterion for the outbound requests to be modified.

FILE = <filename 1..54> / <c-string 1..512 with-low>
Modifies outbound requests which access this file (DVS/POSIX) in the local system.

FILE = *LIBRARY-ELEMENT(...)
Modifies outbound requests which access library members in the local system.

LIBRARY =
Selects the library.

LIBRARY = <u>*ALL</u>
The library name is not selected as a criterion for the outbound requests to be modified

LIBRARY = <filename 1..54>
Outbound requests are to be modified which access this library.

ELEMENT =
Library member.

ELEMENT = *ALL
The name of the library member is not selected as a criterion for the outbound requests to be modified.

ELEMENT = <filename 1..64 without-gen-vers>(...) / <composed-name 1..64 with-under>(...)
Name of the library member.

VERSION =
Version of the member.

VERSION = *ALL
The library member version is not selected as a criterion for the outbound requests to be modified.

VERSION = <text 1..24>
Only outbound requests which access this version of the library member are to be modified.

TYPE =
Type of library member.

TYPE = *ALL
The member type is not selected as a criterion for the outbound requests to be modified.

TYPE = <name 1..8>
Only outbound requests which access library members of this type are to be modified.

MONJV =
Selects any outbound request which is monitored by this job variable.

MONJV = *NONE
No job variable is used as a selection criterion for outbound requests to be changed.

MONJV = <filename 1..54>
The outbound request monitored by this job variable is to be modified.

JV-PASSWORD =
Password which is needed to access the job variable.
If you have already entered the password using the BS2000 command ADD-PASSWORD, you do not need to enter JV-PASSWORD.

JV-PASSWORD = *NONE
The job variable is not password-protected or it does not need to be specified.

JV-PASSWORD = <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
This password is required for the job variable.

JV-PASSWORD = *SECRET
The system prompts you to enter the password. The entry does not appear on the screen. However, the password does not appear on the screen.

QUEUE-POSITION =
New position of the outbound request that is to be modified in the openFT request queue. The position of an FTAM request can only be changed relative to the requests that affect the same FTAM partner.

QUEUE-POSITION = *UNCHANGED
The position of the outbound request in this user's openFT request queue remains unchanged.

QUEUE-POSITION = *FIRST
The outbound request is placed in front of all the other requests of the same priority issued by the user in the openFT request queue.

QUEUE-POSITION = *LAST
The outbound request is placed behind all the other requests of the same priority issued by the user in the openFT request queue.

PRIORITY =
Modifies the priority of the FT request.

PRIORITY = *UNCHANGED
The priority of the FT request remains unchanged.

PRIORITY = *NORMAL
The priority of the FT request is set to the normal value

PRIORITY = *HIGH
The FT request is given a high priority.

PRIORITY = *LOW
The FT request is given a low priority.

Command return codes

(SC2)	SC1	Maincode	Meaning/Guaranteed messages
0	0	CMD0001	There are no requests that meet the specified selection criteria.
32	32	CMD0221	Request rejected. Internal error. Job variable not accessible.
33	32	CMD0221	Request rejected. Internal error.
36	32	CMD0221	Request rejected. Request data inconsistent.
82	32	CMD0221	Internal error. Job variable not accessible.
83	32	CMD0221	Internal error.
36	64	FTR1036	User not authorized for other user IDs.
47	64	FTR1047	Request with the specified transfer ID could not be found.
226	64	FTR2226	Job variable contents inconsistent.
227	64	FTR2227	Job variable not in use by openFT.
228	64	FTR2228	Job variable not found.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

```
/SHOW-FILE-TRANSFER
% TRANS-ID  INI  STATE  PARTNER  DIR   BYTE-COUNT FILE-NAME
% 54483612  LOC   WAIT  UNIX1    FROM  0          FILE1
% 11164324  LOC   WAIT  UNIX2    FROM  0          FILE2

/MODIFY-FILE-TRANSFER SELECT=(FILE=FILE2),QUEUE-POS=*FIRST

/SHOW-FILE-TRANSFER
% TRANS-ID  INI  STATE  PARTNER  DIR   BYTE-COUNT FILE-NAME
% 11164324  LOC   WAIT  UNIX2    FROM  0          FILE2
% 54483612  LOC   WAIT  UNIX1    FROM  0          FILE1
```

5.21 MODIFY-FT-ADMISSION-SET Modify admission set

Note on usage

User group: FTAC user and FTAC administrator

Prerequisite for using this command is the use of openFT-AC.

Functional description

The FTAC user can modify the admission set for his/her own user ID with the MODIFY-FT-ADMISSION-SET command. The FTAC administrator also can modify the admission sets of foreign user IDs. You may access two components of the admission set:

a) You can define a password to be entered for almost all subsequent FTAC commands (except the /SHOW... commands). This prevents other users working with your user ID from entering FTAC commands.

   i It is not possible to have an FTAC password output. If an FTAC user forgets his/her FTAC password, only the FTAC administrator can delete or modify the password.

   ⚠ **WARNING!**
   If the FTAC administrator should assign and subsequently forget a password, openFT-AC must be reinstalled. In this case, all admission profiles and sets are deleted!

   If SECOS is installed, this can be avoided by appointing a new administrator.

b) FTAC users may modify the limit values for the maximum number of security levels that can be reached from their user ID (the MAX-USER-LEVELS) within the range specified by the FTAC administrator. The limit values defined by the FTAC administrator (MAX-ADM-LEVELS) cannot, however, be overridden by the FTAC user. They can simply reduce the limit values since, in the case of FT requests, FTAC performs the admission check on the basis of the smallest value in the admission set. The MAX-USER-LEVELS are only effective if they are lower, i.e. more restrictive, than the MAX-ADM-LEVELS.

   FTAC administrators assign a maximum security level for each of the six basic functions. The user ID associated with the admission set can then use this function with all partner systems with this security level or lower. The owner of the admission set may only increase the degree of restriction.

In addition, the FTAC administrator can delete an admission set from the admission file by entering the default admission set for the user ID in question (MAX-LEVELS=*STD). This is also possible with user IDs which have already been deleted!

Format

```
MODIFY-FT-ADMISSION-SET

 USER-IDENTIFICATION = *OWN / *STD / <alphanum-name 1..8>
,PASSWORD = *NONE / <c-string 1..8 with-low> / <x-string 1..16> / *SECRET
,SELECT-PARAMETER = *ALL
,NEW-PASSWORD = *OLD / *NONE / <c-string 1..8 with-low> / <x-string 1..16> / *SECRET
,MAX-LEVELS = *UNCHANGED / *STD / <integer 0...100> / *PARAMETERS(...)
    *PARAMETERS(...)
    |    OUTBOUND-SEND = *UNCHANGED / *STD / <integer 0...100>
    |   ,OUTBOUND-RECEIVE = *UNCHANGED / *STD / <integer 0...100>
    |   ,INBOUND-SEND = *UNCHANGED / *STD / <integer 0...100>
    |   ,INBOUND-RECEIVE = *UNCHANGED / *STD / <integer 0...100>
    |   ,INBOUND-PROCESSING = *UNCHANGED / *STD / <integer 0...100>
    |   ,INBOUND-MANAGEMENT = *UNCHANGED / *STD / <integer 0...100>
```

Operands

USER-IDENTIFICATION =
User ID whose admission set is to be modified.

USER-IDENTIFICATION = *OWN
The admission set for the user ID which you are currently using is to be modified.

USER-IDENTIFICATION = *STD
The default admission set is to be modified. Only the FTAC administrator can make this entry.

USER-IDENTIFICATION = <alphanum-name 1..8>
The admission set for this user ID is to be modified. The FTAC user can only enter his/her own user ID here.
The FTAC administrator can enter any user ID here.

PASSWORD =
FTAC password which authorizes you to use FTAC commands, if such a password was defined in your admission set. An FTAC password is set with the operand NEW-PASSWORD.

PASSWORD = *NONE
No FTAC password is required for this admission set.

PASSWORD = <c-string 1..8 with-low> / <x-string 1..16>
This password authorizes this user to use FTAC commands.

PASSWORD = *SECRET
The system prompts you to enter the password. However, the password does not appear on the screen.

SELECT-PARAMETER = <u>*ALL</u>
In later openFT-AC versions it will be possible to specify additional selection criteria here.

NEW-PASSWORD =
Changes the FTAC password. If such an FTAC password has already been set, it must be used for almost all FTAC commands on the user ID for this admission set (except: the SHOW... commands). This is done using the parameter PASSWORD in the respective commands.

NEW-PASSWORD = <u>*OLD</u>
The FTAC password remains unchanged.

NEW-PASSWORD = *NONE
No FTAC password is required for the user ID associated with this admission set.

NEW-PASSWORD = <c-string 1..8 with-low> / <x-string 1..16>
Specification of the new FTAC password.

NEW-PASSWORD = *SECRET
The system prompts you to input the password. The input does not appear on the screen, however.

MAX-LEVELS =
You set which security level(s) you can access, with which basic functions, from the user ID of this admission set. Either you can set one security level for all basic functions or different security levels for each basic function.
The MAX-USER-LEVELS for this admission set are set by the FTAC user; the MAX-ADM-LEVELS are set by the FTAC administrator.
FTAC runs authorization checks on the basis of the lowest specified security level. FTAC users may reduce but not increase the values specified for them by the FTAC administrator, see example to SHOW-FT-ADMISSION-SET.

MAX-LEVELS = <u>*UNCHANGED</u>
The security levels set in this admission set are to remain unchanged.

MAX-LEVELS = *STD
For this admission set, the values of the default admission set are valid. The admission set is deleted from the admission file. This is possible if the user ID has already been deleted.

MAX-LEVELS = <integer 0...100>
You can set a maximum security level for all six basic functions. The value 0 means that no file transfer is possible on this user ID until further notice (until the admission set is modified again).

MAX-LEVELS = *PARAMETERS(...)
You can set a maximum security level for each of the basic functions.

OUTBOUND-SEND =
Sets the maximum security level for the basic function “outbound send”. The owner of the admission set can send files to all partner systems whose security level has this value or lower.

OUTBOUND-SEND = <u>*UNCHANGED</u>
The value for OUTBOUND-SEND remains unchanged.

OUTBOUND-SEND = *STD
For OUTBOUND-SEND, the value from the default admission set is used.

OUTBOUND-SEND = <integer 0..100>
For OUTBOUND-SEND, this maximum security level is entered in the admission set.

OUTBOUND-RECEIVE =
Sets the maximum security level for the basic function “outbound receive”. The owner of the admission set can receive files from all partner systems whose security level has this value or lower.

OUTBOUND-RECEIVE = <u>*UNCHANGED</u>
The value for OUTBOUND-RECEIVE remains unchanged.

OUTBOUND-RECEIVE = *STD
For OUTBOUND-RECEIVE, the value from the default admission set is used.

OUTBOUND-RECEIVE = <integer 0..100>
For OUTBOUND-RECEIVE, this maximum security level is entered in the admission set.

INBOUND-SEND =
Sets the maximum security level for the basic function “inbound send”. All partner systems with this security level or lower can request files from the owner of the admission set.

INBOUND-SEND = <u>*UNCHANGED</u>
The value for INBOUND-SEND remains unchanged.

INBOUND-SEND = *STD
For INBOUND-SEND, the value from the default admission set is used.

INBOUND-SEND = <integer 0..100>
For INBOUND-SEND, this maximum security level is entered in the admission set.

INBOUND-RECEIVE =
Sets the maximum security level for the basic function “inbound receive”. All partner systems with this security level or lower may send files to the owner of the admission set.

INBOUND-RECEIVE = _*UNCHANGED_
The value for INBOUND-RECEIVE remains unchanged.

INBOUND-RECEIVE = *STD
For INBOUND-RECEIVE, the value from the default admission set is used.

INBOUND-RECEIVE = <integer 0..100>
For INBOUND-RECEIVE, this maximum security level is entered in the admission set.

INBOUND-PROCESSING =
Sets the maximum security level for the basic function “inbound processing”. All partner systems which have this security level or lower may include follow-up processing in their system as part of an FT request.

INBOUND-PROCESSING = _*UNCHANGED_
The value for INBOUND-PROCESSING remains unchanged.

INBOUND-PROCESSING = *STD
For INBOUND-PROCESSING, the value from the default admission set is used.

INBOUND-PROCESSING = <integer 0..100>
For INBOUND-PROCESSING, this maximum security level is entered in the admission set.

INBOUND-MANAGEMENT =
Sets the maximum security level for the basic function “inbound file management”. All partner systems with this security level or lower may include the modification of file attributes and the querying of directories as part of their FT request.

INBOUND-MANAGEMENT = _*UNCHANGED_
The value for INBOUND-MANAGEMENT remains unchanged.

INBOUND-MANAGEMENT = *STD
For INBOUND-MANAGEMENT, the value from the default admission set is used.

INBOUND-MANAGEMENT = <integer 0..100>
For INBOUND-MANAGEMENT, this maximum security level is entered in the admission set.

Example

Jack John, the FTAC administrator of the Dack Bank, wishes set up the admission set for his employee Steven, such that Steven

– can send files to partner systems with the security level of 10 or lower (basic function “outbound send”),

– can request files from partner systems with the security level of 10 or lower (basic function “outbound receive”).

He wants all partner systems to be able send files to and request files from the user ID STEVEN. Therefore he sets the security level for INBOUND-SEND and INBOUND-RECEIVE to 100.

Jack does not wish to permit follow-up processing to be initiated from external partners, since he is too stingy to want to make his resources available to others. Therefore, he sets INBOUND-PROCESSING and INBOUND-FILEMANAGEMENT at 0. Since these values are set in the default admission set for the Dack Bank, these specifications are used for *STD. No FTAC password is defined.

The long form of the required command is as follows:

```
/MODIFY-FT-ADMISSION-SET USER-IDENTIFICATION=STEVEN,             -
/                        MAX-LEVELS=(OUTBOUND-SEND=10,             -
/                                    OUTBOUND-RECEIVE=10,        -
/                                    INBOUND-SEND=100,           -
/                                    INBOUND-RECEIVE=100,        -
/                                    INBOUND-PROCESSING=*STD,    -
/                                    INBOUND-MANAGEMENT=*STD)
```

A possible short form of this command would be:

```
/MOD-FT-ADM STEVEN,MAX-LEV=(10,10,100,100,*STD,*STD)
```

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	FTC0050	The set security level exceeds the administrator‘s limit and will remain invalid until the administrator’s limit is raised accordingly.
0	64	FTC0150	The authorization password is missing.
0	64	FTC0151	Only the administrator or owner is permitted to make this modification.
0	64	FTC0152	The user ID entered is not the user‘s own user ID.
0	64	FTC0175	The operand “NEW-PASSWORD” may not be entered for *STD.
0	64	FTC0176	The user ID entered does not exist in the system.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, seesection “Command return codes” on page 133

5.22 MODIFY-FT-INSTANCE Modify an openFT instance

Note on usage

User group: FT administrator

Functional description

Using this command, you can modify the characteristics of an instance (name, automatic start of openFT).

MODIFY-FT-INSTANCE may only be set up if openFT is not started in this instance, (STARTED=*NO is displayed in the SHOW-FT-INSTANCE command).

> **WARNING!**
>
> The instance may not be renamed; this is because system resources that contain the instance name may still be occupied even though openFT has been terminated. That is the case, for example, if requests with pre- or post-processing are still entered under this instance.

Format

MODIFY-**FT**-**INST**ANCE
NAME = <alphanum-name 1..8> ,**NEW-NAME** = ***UNCHA**NGED / <alphanum-name 1..8> ,**AUTO**MATIC-**START** = ***UNCHA**NGED / ***ON** / ***OFF**

Operands

NAME = <alphanum-name 1..8>
Name of the openFT instance that is to be modified.

NEW-NAME = *UNCHANGED
The instance name remains unchanged.

NEW-NAME = <alphanum-name 1..8>
The new instance name. This name must be identical on all the computers on which this instance is to be used.

AUTOMATIC-START =
This is specified if, after loading the instance, openFT is automatically started in this instance.

AUTOMATIC-START = *UNCHANGED
The previous setting remains unchanged.

AUTOMATIC-START = *OFF
After loading the instance, openFT is not started.

AUTOMATIC-START = *ON
After each loading of the instance, a START-FT command is also implicitly executed in this instance. In this way, it is possible to work with openFT immediately after loading. All the components that are available for the standard instance are also started such as, for example, openFT-AC and openFT-FTAM.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
25	64	FTR1025	Instance does not exist.
26	64	FTR1026	Instance must not be modified.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section "Command return codes" on page 133

5.23 MODIFY-FT-KEY Modify key

Note on usage

User group: FT administrator

Alias name: FTMODKEY

Functional description

You can use the MODIFY-FT-KEY command to modify the expiration date and authentication level of keys that are used for the authentication of partner systems. The changes are stored in the relevant key file.

Once the expiration date of a key has been reached, authentication using this key is rejected. However, you can still modify the expiration date after the key’s validity dateb has expired, e.g. in order to temporarily re-enable a key so that a current key can be transferred securely.

Format

MODIFY-**FT**-**KEY / FTMODKEY**
PARTNER-**NAME** = ***ALL** / <name 1..8> ,**AUTH**ENTICATION-**LEV**EL = ***UNCHA**NGED / <integer 1..2> ,**EXP**IRATION-**DATE** = ***UNCHA**NGED / *NONE / <date 8..10>

Operands

PARTNER-NAME =
Specifies the partner whose key is to be modified.

PARTNER-NAME = *ALL
The installed keys of all partner systems are modified.

PARTNER-NAME = <name 1..8>
Name of the partner whose key is modified.

AUTHENTICATION-LEVEL =
Species the authentication level for the key or keys.

AUTHENTICATION-LEVEL = *UNCHANGED
The authentication level remains unchanged.

AUTHENTICATION-LEVEL = 1
The authentication level for the partner or partners is set to 1. This corresponds to the options available up to openFT V11.0A.

If the partner system is subsequently authenticated at level 2, then the entry AUTHENTICATION-LEVEL=2 is automatically recorded in its key file.

AUTHENTICATION-LEVEL = 2
The partner system supports the level 2 authentication procedure introduced in openFT V11.0B . Level 1 authentication attempts are rejected.

EXPIRATION-DATE =
Specifies the expiration date of the key or keys.

EXPIRATION-DATE = *UNCHANGED
The expiration date remains unchanged.

EXPIRATION-DATE = *NONE
No expiration date for the key or keys.

EXPIRATION-DATE = <date 8..10>
Expiration date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g.. 2012-12-31 or 12-12-31 for December 31, 2012. The key or keys can be used for authentication at the latest up until the time 00:00 on the specified date.

Command return codes

(SC2)	SC1	Maincode	Bedeutung
0	0	CMD0001	The key has been modified
83	32	CMD0221	Internal error
35	64	FTR1035	Command only permissible for FT administrator
76	64	FTR1076	Selected key file not found
2	0	FTR1087	Key expired

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.24 MODIFY-FT-OPTIONS Modify operating parameters

Note on usage

User group: FT administrator

Alias name: FTMODOPT

Functional description

The MODIFY-FT-OPTIONS command is used to modify one or more operating parameters of the local system. The relationships between the different operating parameters are explained in section "Optimizing the operating parameters" on page 341.

After setting up an instance that is not working via the standard host, a host must be configured for this instance using the MODIFY-FT-OPTIONS command. Only then can openFT be started for the first time in this instance. Using MODIFY-FT-OPTIONS, an instance ID which is unique throughout the network must, if necessary, be set before the initial startup..

The MODIFY-FT-OPTIONS command also enables you to do the following:

- Activate and deactivate the FT trace function, SNMP traps and console and ADM traps
- Control FT logging, monitoring and user data encryption

i Any unspecified operating parameters remain unchanged. The current operating parameters can be queried at any time using the SHOW-FT-OPTIONS command (see page 351).

Format

(part 1 of 3)

MODIFY-**FT**-**OPT**IONS / **FTMODOPT**

PROCESS-**LIM**IT = ***UNCHA**NGED / <integer 1..32> / ***NONE**

,**CONN**ECTION-**LIM**IT = ***UNCHA**NGED / <integer 1..255>

,**REQ**UEST-**WAIT**-LEVEL = ***UNCHA**NGED

,**PACING** = ***UNCHA**NGED

,**TRANS**PORT-**UNIT**-SIZE = ***UNCHA**NGED / <integer 512..65535>

,**SEC**URITY-**LEV**EL = ***UNCHA**NGED / ***BY**-**PART**NER-**ATTR**IBUTES / <integer 1..100>

,**PART**NER-**CHECK** = ***UNCHA**NGED / ***STD** / ***TRANS**PORT-**ADDR**ESS

,**TRACE** = ***UNCHA**NGED / ***ON** / ***OFF** / ***CHA**NGE-FILES / ***PAR**AMETERS(...)

  ***PAR**AMETERS(...)

   | **SWITCH** = ***UNCHA**NGED / ***ON** / ***OFF** / ***CHA**NGE-FILES

   | ,**PART**NER-**SEL**ECTION = ***UNCHA**NGED / ***ALL** / ***NONE** / list-poss(4): ***OPENFT** / ***FTAM** / ***FTP** / ***ADM**

   | ,**REQ**UEST-**SEL**ECTION = ***UNCHA**NGED / ***ALL** / list-poss(2): *ONLY-**SYNC** / *ONLY-**ASYNC** / *ONLY-**LOC**AL / *ONLY-**REM**OTE

   | ,**OPT**IONS = ***UNCHA**NGED / ***NONE** / list-poss(1): ***NO**-**BULK**-DATA

,**LOGG**ING = ***UNCHA**NGED / ***CHA**NGE-FILES / ***SEL**ECT(...)

  ***SEL**ECT(...)

   | **TRANS**FER-**FILE** = ***UNCHA**NGED / ***OFF** / ***ON** / ***FAIL**URE

   | ,**FTAC** = ***UNCHA**NGED / ***ON** / ***REJ**ECTED / ***MOD**IFICATIONS

   | ,**ADM** = ***UNCHA**NGED / ***OFF** / ***ON** / ***FAIL**URE/ ***MOD**IFICATIONS

,**MAX-INB**OUND-**REQ**UEST = ***UNCHA**NGED

,**REQ**UEST-**LIM**IT = ***UNCHA**NGED / <integer 2..32000>

,**MAX-REQ**UEST-**LIFE**TIME = ***UNCHA**NGED / ***UNLIM**ITED / <integer 1..400>

,**SNMP-TRAPS** = ***UNCHA**NGED / ***ALL** / ***NONE** / ***PAR**AMETERS(...)

  ***PAR**AMETERS(...)

   | **SUBSYS**TEM-**STATE** = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**FT-STATE** = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**PART**NER-**STATE** = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**PART**NER-**UNREA**CHABLE = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**R**EQUEST-**Q**UEUE-**STATE** = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**TRANS**FER-**SUCC**ESS = ***UNCHA**NGED / ***OFF** / ***ON**

   | ,**TRANS**FER-**FAIL**URE = ***UNCHA**NGED / ***OFF** / ***ON**

(part 2 of 3)

```
,CONSOLE-TRAPS =  *UNCHANGED / *ALL / *NONE / *PARAMETERS(...)

   *PARAMETERS(...)
   |  SUBSYSTEM-STATE = *UNCHANGED / *OFF / *ON
   | ,FT-STATE = *UNCHANGED / *OFF / *ON
   | ,PARTNER-STATE = *UNCHANGED / *OFF / *ON
   | ,PARTNER-UNREACHABLE = *UNCHANGED / *OFF / *ON
   | ,REQUEST-QUEUE-STATE = *UNCHANGED / *OFF / *ON
   | ,TRANSFER-SUCCESS = *UNCHANGED / *OFF / *ON
   | ,TRANSFER-FAILURE = *UNCHANGED / *OFF / *ON

,HOST-NAME = *UNCHANGED / <alphanum-name 1..8>

,IDENTIFICATION = *UNCHANGED / <c-string 1..64 with-low> / <composed-name 1..64>

,KEY-LENGTH = *UNCHANGED / 0 / 768 / 1024 / 2048

,OPENFT-APPLICATION = *UNCHANGED / *STD / <text 1..24>

,OPENFT-STD = *UNCHANGED / *STD /  <integer 1..65535>

,FTAM-APPLICATION = *UNCHANGED / *STD / <text 1..40>

,FTP-PORT = *UNCHANGED / *NONE / *STD / <integer 1..65535>

,DYNAMIC-PARTNERS = *UNCHANGED / *OFF / *ON

,ADM-PORT = *UNCHANGED / *STD / <integer 1..65535>

,ACTIVE-APPLICATIONS = *UNCHANGED / *ALL / *NONE / list-poss(3): *OPENFT / *ADM / *FTP

,ADM-CONNECTION-LIMIT = *UNCHANGED / <integer 1..255>

,MONITORING  = *UNCHANGED / *ON / *OFF / *PARAMETERS(...)

   *PARAMETERS(...)
   |  SWITCH = *UNCHANGED / *ON / *OFF
   | ,PARTNER-SELECTION = *UNCHANGED / *ALL / *NONE / list-poss(3): *OPENFT / *FTAM / *FTP
   | ,REQUEST-SELECTION = *UNCHANGED / *ALL / list-poss(2): *ONLY-SYNC / *ONLY-ASYNC /
   |                                 *ONLY-LOCAL / *ONLY-REMOTE
```

(part 3 of 3)

```
,ADM-TRAPS = *UNCHANGED / *NONE / *PARAMETERS(...)
   *PARAMETERS(...)
   |  DESTINATION = *UNCHANGED / *NONE / *PARAMETERS(...)
   |     *PARAMETERS(...)
   |     |  PARTNER = *UNCHANGED / <text 1..200 with-low>
   |     |  ,TRANSFER-ADMISSION = *UNCHANGED / <alphanum-name 8..32> /
   |     |                          <c-string 8..32 with-low> / <x-string15..64> / *SECRET
   |  ,SELECTION = *UNCHANGED / *ALL/ *NONE / *PARAMETERS(...)
   |     *PARAMETERS(...)
   |     |  ,FT-STATE = *UNCHANGED / *OFF / *ON
   |     |  ,FT-STATE = *UNCHANGED / *OFF / *ON
   |     |  ,PARTNER-STATE = *UNCHANGED / *OFF / *ON
   |     |  ,PARTNER-UNREACHABLE = *UNCHANGED / *OFF / *ON
   |     |  ,REQUEST-QUEUE-STATE = *UNCHANGED / *OFF / *ON
   |     |  ,TRANSFER-SUCCESS = *UNCHANGED / *OFF / *ON
   |     |  ,TRANSFER-FAILURE = *UNCHANGED / *OFF / *ON
,ENCRYPTION-MANDATORY = *UNCHANGED / *NO / list-poss(2): *INBOUND / *OUTBOUND
,DELETE-LOGGING = *UNCHANGED / *PARAMETERS(...)
   *PARAMETERS(...)
   |  SWITCH = *UNCHANGED / *ON / *OFF
   |  ,RETENTION-PERIOD = *UNCHANGED / <integer 0..999 days>
   |  ,REPEAT = *UNCHANGED / *DAILY / *WEEKLY(...) / *MONTHLY(...)
   |     *WEEKLY(...)
   |     |  ON = *SUNDAY / *MONDAY / *TUESDAY / *WEDNESDAY / THURSDAY / *FRIDAY /
   |     |        *SATURDAY
   |     *MONTHLY(...)
   |     |  ON = 1 / <integer 1..31>
   |  ,DELETE-TIME = *UNCHANGED / <time 1..8>
```

Operands

PROCESS-LIMIT =

Maximum number of tasks that can be reserved simultaneously for the execution of file transfer requests.

Default setting following installation: 2

PROCESS-LIMIT = *UNCHANGED

PROCESS-LIMIT is not changed, default value.

PROCESS-LIMIT = <integer 1..32>
PROCESS-LIMIT can have any value between 1 and 32.

PROCESS-LIMIT = *NONE
A server task is created for each new connection. PROCESS-LIMIT is therefore restricted by CONNECTION-LIMIT.

CONNECTION-LIMIT =
Maximum number of transport connections that can be reserved for the execution of FT requests. This limit does not include file management requests and synchronous requests. The maximum number of transport connections cannot be exceeded, not even if there are many high-priority file transfer requests to be executed. Since only one request can be processed at a time per transport connection, CONNECTION-LIMIT is also the maximum number of requests which a system can process simultaneously. One third of the transport connections defined by CONNECTION-LIMIT are reserved for requests from the remote system, and another third for requests submitted in the local system. The remaining third are available for both local and remote requests. This prevents locally submitted requests from blocking the system against requests from remote systems. If CONNECTION-LIMIT is less than 3, no transport connections are reserved.

Default setting following installation: 8

CONNECTION-LIMIT = *UNCHANGED
The CONNECTION-LIMIT value is not changed, default value.

CONNECTION-LIMIT = <integer 1..255>
CONNECTION-LIMIT can have any value between 1 and 255.

REQUEST-WAIT-LEVEL = *UNCHANGED
The value for REQUEST-WAIT-LEVEL is unchanged.

PACING = *UNCHANGED
This parameter is only supported for reasons of compatibility an cannot be modified.

TRANSPORT-UNIT-SIZE =
Maximum size of a transport unit in bytes.

Default setting following installation: 65535 bytes

TRANSPORT-UNIT-SIZE = *UNCHANGED
The current value size of a transport unit in bytes is unchanged.

TRANSPORT-UNIT-SIZE = <integer 512..65535>
TRANSPORT-UNIT-SIZE can assume any value between 512 and 65535.
It is recommended that you use value 65535.
TRANSPORT-UNIT-SIZE does not affect links with FTAM partners.

SECURITY-LEVEL =
This parameter need only be specified when FTAC functionality is used. An important part of the access protection functions provided by this product is based on the allocation of a security level to each partner. These security levels are designated using integers. The FT administrator can define a global value. This security level applies to all partner systems in the partner list that are not explicitly assigned their own security levels when entered.

Default setting following installation: *BY-PARTNER-ATTRIBUTES

SECURITY-LEVEL = *UNCHANGED
The security level is unchanged.

SECURITY-LEVEL = *BY-PARTNER-ATTRIBUTES
If you set the operand to *BY-PARTNER-ATTRIBUTES then the security level is defined automatically. This setting assigns partners that are authenticated by openFT the security level 10. Partners that are known in BCAM (i.e. they are addressed via their BCAM names) are assigned the security level 90. All other partners are assigned security level 100.

SECURITY-LEVEL = <integer 1..100>
SECURITY-LEVEL can assume any value between 1 and 100. If FTAC functionality is to be used, remember that 1 is the lowest level of security, offering the least protection. This is sufficient if you do not wish to further differentiate your remote systems; otherwise, a higher value should be defined. The allocation of different security levels is particularly meaningful if the authentication check is activated.

PARTNER-CHECK =
Activates the extended authentication check. When using expanded sender checking, not only the partner identification is checked, but also the transport address. PARTNER-CHECK only affects named openFT partners that are not authenticated in the local system the (see the section “Authentication” on page 53).

This option has no meaning for FTAM and FTP partners. For them only the transport address (not the identification) is checked.

The globally set expanded sender checking can be modified for specific partners, see the operand PARTNER-CHECK for the ADD-FT-PARTNER and MODIFY-FT-PARTNER commands.

Default setting following installation: *STD

PARTNER-CHECK = *UNCHANGED
The existing value is retained.

PARTNER-CHECK = *STD
If dynamic partners are prohibited (DYNAMIC-PARTNERS=*OFF), a check is performed to determine whether the partner is entered in the partner list as a partner system with his/her instance identification, and only then will the file transfer be allowed.

If dynamic partners are permitted (DYNAMIC-PARTNERS=*ON), transfers are also permitted from partners that are accessed only using their address or are not entered in the partner list at all.

PARTNER-CHECK = *TRANSPORT-ADDRESS
Extended authentication check. In addition to checking whether the partner is entered in its own partner list as a partner system, it is checked whether the transport address under which the partner logs on matches the transport address entered in the partner list for the partner system. In the SHOW-FT-OPTIONS command then PARTNER-CHECK = ADDR is output.
This setting has no significance for dynamic partners and FTAM or FTP partners.

TRACE =
Defines the settings for the FT trace functions.

Default setting following installation: *OFF

TRACE = <u>*UNCHANGED</u>
The existing FT trace functions remain unchanged.

TRACE = *ON
Switches the FT trace functions on.

TRACE = *OFF
Switches the FT trace functions off.

TRACE = *CHANGE-FILES
Switches to a new trace file. This allows a continuous trace to be created across several files to prevent a single trace file from becoming too large.

TRACE = *PARAMETERS(...)
Option that is to be applied when writing the trace.

SWITCH =
Deactivates the FT trace functions for the selected partners.
Default setting following installation: *OFF

SWITCH = <u>*UNCHANGED</u>
The previous value is unchanged.

SWITCH = *ON
Activates the FT trace functions.

SWITCH = *OFF
Deactivates the FT trace functions.

SWITCH = *CHANGE-FILES
Switches to a new trace file. This allows a continuous trace to be created across several files to prevent a single trace file from becoming too large.

PARTNER-SELECTION =
Selects the partners that are to be traced. The selection made here can be modified with the TRACE operand of the MODIFY-FT-PARTNER command.
Default setting following installation: *ALL

PARTNER-SELECTION = *UNCHANGED
The previous value is unchanged.

PARTNER-SELECTION = *ALL
All the partners are selected for tracing.

PARTNER-SELECTION = *NONE
No partner is selected for tracing. Only those partners are traced which have been selected for tracing with the TRACE operand of the MODIFY-FT-PARTNER command.

PARTNER-SELECTION = *OPENFT
All partners which are addressed via the openFT protocol are selected for tracing.

PARTNER-SELECTION = *FTAM
All partners which are addressed via the FTAM protocol are selected for tracing.

PARTNER-SELECTION = *FTP
All partners which are addressed via the FTP protocol are selected for tracing.

PARTNER-SELECTION = *ADM
All administration partners are selected for monitoring.

REQUEST-SELECTION =
Selects the request types that are to be traced.
Default setting following installation: *ALL

REQUEST-SELECTION = *UNCHANGED
The previous value is unchanged.

REQUEST-SELECTION = *ALL
All the requests are selected for tracing.

REQUEST-SELECTION = *ONLY-SYNC
All synchronous requests are selected for tracing. Synchronous requests are always issued locally.

REQUEST-SELECTION = *ONLY-ASYNC
All asynchronous requests are selected for tracing. Requests issued remotely are always regarded as asynchronous.

REQUEST-SELECTION = *ONLY-LOCAL
All locally submitted requests are selected for tracing.

REQUEST-SELECTION = *ONLY-REMOTE
All remotely submitted requests are selected for tracing.

OPTIONS =
Controls the options for the trace functions.
Default setting following installation: *NONE

OPTIONS = *UNCHANGED
The previous value is unchanged.

OPTIONS = *NONE
No options are selected for the trace functions.

OPTIONS = *NO-BULK-DATA
If file contents (bulk data) are transferred with a protocol element and multiple trace records with the same protocol element occur in succession then only the first of these records is written to the trace file. This reduces the volume of the trace file.

LOGGING =
Switches the logging functions.

LOGGING = *UNCHANGED
The existing logging functions remain unchanged.

LOGGING = *CHANGE-FILES
The log file is changed.
The new log file is created under the name SYSLOG.Lyymmdd.Lhhmmss. *yymmdd* is the date (year, month, day) and *hhmmss* is the time (hour, minute, second in GMT) on/at which the file was created.
The old log file is closed and remains stored as an offline log file.

LOGGING = *SELECT(...)
Controls logging for FT, FTAC and administration functions.
Default setting following installation: *ON for all types of log records

TRANSFER-FILE = *UNCHANGED
The previous settings for FT logging remain unchanged.

TRANSFER-FILE = *OFF
Switches the FT logging functions off.

TRANSFER-FILE = *ON
Switches the FT logging functions on.

TRANSFER-FILE = *FAILURE
Only failed requests are written to the logging file.

FTAC = *UNCHANGED
The previous settings for FTAC logging remain unchanged.

FTAC = *ON
Switches the FTAC logging functions on.

FTAC = *REJECTED
All requests rejected by FTAC are logged.

FTAC = *MODIFICATIONS
All modifying requests are logged.

ADM = *UNCHANGED
The previous settings for administration logging remain unchanged.

ADM = *OFF
Deactivates administration logging.

ADM = *ON
Activates administration logging.

ADM = *FAILURE
Only failed administration requests are written to the log file.

ADM = *MODIFICATIONS
Only administration requests that modify data are written to the log file.

MAX-INBOUND-REQUEST = *UNCHANGED
MAX-INBOUND-REQUEST is now only supported for reasons of compatibility.

REQUEST-LIMIT =
Changes the number of requests which can be saved in the request queue.
Although it is logically possible to reduce the size of the request queue, this does not result in any memory being freed but only reduces the size of the internal queue. To free memory, it is necessary to end the FT subsystem, delete the request queue (SYSRQF) and then restart openFT.

Default setting following installation: 2000

REQUEST-LIMIT = *UNCHANGED
The previous value remains unchanged.

REQUEST-LIMIT = <integer 2..32000>
The maximum number of requests which can be saved in the request queue is changed to the value specified.

MAX-REQUEST-LIFETIME =
Limits the lifetime of FT requests in the request file. The maximum lifetime applies to inbound and outbound requests and is specified in days. The default value when a new request file is generated is 30 days.
The maximum lifetime does not apply to requests that have been transferred from an earlier request file as part of a version change. Such requests still have to be terminated using the CANCEL-FILE-TRANSFER command.

Default setting following installation: 30 days

MAX-REQUEST-LIFETIME = *UNCHANGED
The previous value remains unchanged.

MAX-REQUEST-LIFETIME = *UNLIMITED
The lifetime of FT requests is unlimited.

MAX-REQUEST-LIFETIME = <integer 1..400>
The maximum lifetime for FT requests may have a value of between 1 and 400 days.

SNMP-TRAPS =
Activates or deactivates specific SNMP traps. SNMP traps are generated to indicate specific events which are routed by the FT subagent to an SNMP Management Station if one is in use.
Default setting following installation: *NONE

SNMP-TRAPS = *UNCHANGED
The previous value is unchanged.

SNMP-TRAPS = *NONE
Deactivates all SNMP traps.

SNMP-TRAPS = *ALL
Activates all SNMP traps.

SNMP-TRAPS = *PARAMETERS(...)
Activates or deactivates selected SNMP traps. For further information, please refer to section “SNMP management for openFT” on page 70.

SUBSYSTEM-STATE =
Controls the output of SNMP traps concerning the status of the openFT subsystem.
Default setting following installation: *OFF

SUBSYSTEM-STATE = *UNCHANGED
The previous value is unchanged.

SUBSYSTEM-STATE = *OFF
No SNMP traps concerning the status of the openFT subsystem are output.

SUBSYSTEM-STATE = *ON
SNMP traps concerning the status of the openFT subsystem are output.

FT-STATE =
Controls trap transmission on START-FT / STOP-FT or abnormal FT termination.
Default setting following installation: *OFF

FT-STATE = *UNCHANGED
The previous value is unchanged.

FT-STATE = *OFF
Deactivates the FT-STATE traps.

FT-STATE = *ON
Activates the FT-STATE traps.

PARTNER-STATE =
Controls trap transmission when the status of FT partners changes.
Default setting following installation: *OFF

PARTNER-STATE = <u>*UNCHANGED</u>
The previous value is unchanged.

PARTNER-STATE = *OFF
Deactivates the PARTNER-STATE traps.

PARTNER-STATE = *ON
Activates the PARTNER-STATE traps.

PARTNER-UNREACHABLE =
Controls transmission of the trap that indicates if a partner cannot be accessed.
Default setting following installation: *OFF

PARTNER-UNREACHABLE = <u>*UNCHANGED</u>
The previous value is unchanged.

PARTNER-UNREACHABLE = *OFF
Deactivates the “partner unreachable” trap.

PARTNER-UNREACHABLE = *ON
Activates the “partner unreachable” trap.

REQUEST-QUEUE-STATE =
Controls the transmission of traps when the request queue is more than 85% or less than 80% full.
Default setting following installation: *OFF

REQUEST-QUEUE-STATE = <u>*UNCHANGED</u>
The previous value is unchanged.

REQUEST-QUEUE-STATE = *OFF
Deactivates the request queue fill level traps.

REQUEST-QUEUE-STATE = *ON
Activates the request queue fill level traps.

TRANSFER-SUCCESS =
Controls the transmission of the trap that indicates that an FT request has been successfully concluded.
Default setting following installation: *OFF

TRANSFER-SUCCESS = <u>*UNCHANGED</u>
The previous value is unchanged.

TRANSFER-SUCCESS = *OFF
Deactivates the TRANSFER-SUCCESS trap.

TRANSFER-SUCCESS = *ON
Activates the TRANSFER-SUCCESS trap.

TRANSFER-FAILURE =
Controls the transmission of the trap that indicates that an FT request has been aborted.
Default setting following installation: *OFF

TRANSFER-FAILURE = <u>*UNCHANGED</u>
The previous value is unchanged.

TRANSFER-FAILURE = *OFF
Deactivates the TRANSFER-FAILURE trap.

TRANSFER-FAILURE = *ON
Activates the TRANSFER-FAILURE trap.

CONSOLE-TRAPS =
Activates or deactivates console traps.
By default, these trap messages are not displayed at the console. However, they are logged in the CONSLOG file.
They can therefore cause storage problems on systems with high request volumes.
By default, the output of console traps is activated.
Default setting following installation: *OFF

CONSOLE-TRAPS = <u>*UNCHANGED</u>
The previous value is unchanged.

CONSOLE-TRAPS = *ALL
The FTR03XX console messages are output by openFT. They always appear in the CONSLOG file. However, they are only output to the console if they are explicitly requested using the following command, e.g.:

```
/MOD-MSG-SUBSCRIPTION ADD-MSG-ID=(FTR0301,FTR0307,FTR0340,FTR0341)
```

CONSOLE-TRAPS = *NONE
The FTR03XX console messages are not output.

CONSOLE-TRAPS = *PARAMETERS(...)
Explicit specification of the events for which FTR03XX console messages are output.

SUBSYSTEM-STATE =
Controls the output of console messages concerning the status of the openFT subsystems.
Default setting following installation: *OFF

SUBSYSTEM-STATE = *UNCHANGED
The previous value is unchanged.

SUBSYSTEM-STATE = *OFF
No console messages concerning the status of the openFT subsystem are output.

SUBSYSTEM-STATE = *ON
Console messages concerning the status of the openFT subsystem are output.

FT-STATE =
Controls the output of console messages concerning the status of the openFT control process.
Default setting following installation: *OFF

FT-STATE = *UNCHANGED
The previous value is unchanged.

FT-STATE = *OFF
No console messages concerning the status of the openFT control process are output.

FT-STATE = *ON
Console messages concerning the status of the openFT control process are output.

PARTNER-STATE =
Controls the output of console messages concerning the status of the partner systems.
Default setting following installation: *OFF

PARTNER-STATE = *UNCHANGED
The previous value is unchanged.

PARTNER-STATE = *OFF
No console messages concerning the status of partner systems are output.

PARTNER-STATE = *ON
Console messages concerning the status of partner systems are output.

PARTNER-UNREACHABLE =
Controls the output of console messages if partner systems cannot be accessed.
Default setting following installation: *OFF

PARTNER-UNREACHABLE = *UNCHANGED
The previous value is unchanged.

PARTNER-UNREACHABLE = *OFF
No console messages are output if partner systems cannot be accessed.

PARTNER-UNREACHABLE = *ON
Console messages are output if partner systems cannot be accessed.

REQUEST-QUEUE-STATE =
Controls the output of console messages concerning the status of the request queue.

Default setting following installation: *OFF

REQUEST-QUEUE-STATE = *UNCHANGED
The previous value is unchanged.

REQUEST-QUEUE-STATE = *OFF
No console messages concerning the status of the request queue are output.

REQUEST-QUEUE-STATE = *ON
Console messages concerning the status of the request queue are output.

TRANSFER-SUCCESS =
Controls the output of console messages when a request is terminated successfully.
Default setting following installation: *OFF

TRANSFER-SUCCESS = *UNCHANGED
The previous value is unchanged.

TRANSFER-SUCCESS = *OFF
No console messages are output if a request is terminated successfully.

TRANSFER-SUCCESS = *ON
Console messages are output if a request is terminated successfully.

TRANSFER-FAILURE =
Controls the output of console messages when a request fails.
Default setting following installation: *OFF

TRANSFER-FAILURE = *UNCHANGED
The previous value is unchanged.

TRANSFER-FAILURE = *OFF
No console messages are output if a request fails.

TRANSFER-FAILURE = *ON
Console messages are output if a request fails.

HOST-NAME =
For using the openFT instance concept: Here you can set the BCAM host to which the transport system calls are made.

Default setting following installation: *NONE

HOST-NAME = *UNCHANGED
The setting for the BCAM host remains unchanged.

HOST-NAME = <alphanum-name 1..8>
The name of the BCAM host via which the requests are processed. The result of this is that requests of an openFT instance are always processed via the same network address, irrespective of the real host. If an instance is to run on a virtual host, then the host name must be entered here before the first START-FT. Later, the host name should not be changed. It may not be changed if requests are present in the request file of this instance.

IDENTIFICATION =
Local instance ID of your openFT instance. With the aid of this instance ID, openFT partners as of V8.1 manage the resources for your openFT instance.

The instance ID must be unique, network-wide and must not be case-sensitive. An instance ID may consist of alphanumeric characters or special characters and may have a maximum length of 64 characters. It is advisable only to use the special characters ".", "-", ":" or "%". The initial character must be alphanumeric or the special character "%". The character "%" may only be used as an initial character. The character "." must be followed by an alphanumeric character. For further details on assigning instance identifications, see section "Instance identifications" on page 55.

Default setting following installation: When an instance is installed for the first time, the BCAM name of the real host under which their instance operates is entered as the default setting. If another identification is to be used for operation then this must be configured with MODIFY-FT-OPTIONS .

IDENTIFICATION = *UNCHANGED
The instance ID remains unchanged.

IDENTIFICATION = <c-string 1..64 with-low> / <composed-name 1..64>
The instance ID is set to this value.

KEY-LENGTH =
Length of the RSA key used for encryption. This key is used only to encrypt the AES key which is agreed on between the partners (or the DES key up to and including openFT V7.0). openFT uses the AES key to encrypt the request description data and possibly also the file contents.
Default setting following installation: 2048

KEY-LENGTH = *UNCHANGED
The previous value is unchanged.

KEY-LENGTH = 0
Explicitly disables encryption.

KEY-LENGTH = 768 / 1024 / 2048
Key length in bits.

OPENFT-APPLICATION =
Specifies a port number and/or a transport selector for the local openFT server. Use this function carefully as it will be more difficult for the openFT partners to address the local system if the port number or transport selector differ from the default values!
Default setting following installation: *STD

OPENFT-APPLICATION = *UNCHANGED
The previous value is unchanged.

OPENFT-APPLICATION = *STD
The port number and transport selector are set to the default value, i.e.:
Port number: 1100
Transport selector: $FJAM in EBCDIC code, followed by three spaces.

OPENFT-APPLICATION = <text 1..24>
Valid port number and/or a transport selector in the form [<port number>].[tsel].

OPENFT-STD =
Port number other than the default when addressing openFT partners via their host names. Use this function carefully, as changing the port number from the default value means that it will no longer be possible to reach openFT partners which use the default port number and are addressed via the host name!
Default setting following installation: *STD

OPENFT-STD = *UNCHANGED
The previous value is unchanged.

OPENFT-STD = *STD
The port number is set to the default value 1100.

OPENFT-STD = <integer 1..65535>
Valid port number.

FTAM-APPLICATION =
Specifies a port number other than the default for the local FTAM server. You can also specify a transport selector which differs from the default $FTAM plus a session and presentation selectors.
Use this function carefully, as changing the port number and/or selectors from the default value will make it more difficult for the FTAM partners to address the local system!
Default setting following installation: *STD

FTAM-APPLICATION = *UNCHANGED
The previous value is unchanged.

FTAM-APPLICATION = *STD
The port number is set to the default value 4800. The transport selector is reset to the default value $FTAM (in EBCDIC, followed by three blanks). Session and presentation selectors are reset to the empty format.

FTAM-APPLICATION = <text 1..40>
Specifies a valid port number, optionally together with selectors in the format <port number>.[transport selector].[session selector].[presentation selector].

FTP-PORT =
This option allows you to specify the port number used by FTP.
Default setting following installation: 21

FTP-PORT = <u>*UNCHANGED</u>
The previous value is unchanged.

FTP-PORT = *NONE
No port number is defined. The FTP server is deactivated, i.e. it cannot accept any inbound FTP requests. This setting is only supported for reasons of compatibility. Instead, you should use the operand ACTIVE-APPLICATIONS to activate and deactivate the inbound FTP server.

FTP-PORT = *STD
The port number is set to the default value 21.

FTP-PORT = <integer 1..65535>
Valid port number.

DYNAMIC-PARTNERS =
Specifies whether dynamic partners are permitted.
Default setting following installation: *ON

DYNAMIC-PARTNERS = <u>*UNCHANGED</u>
The previous value is unchanged.

DYNAMIC-PARTNERS = *OFF
Dynamic partners are not permitted. This means that it is only possible to access partner systems which are entered in the partner list and are addressed via the partner name. Transfer requests with partners which are not entered in the partner list or are entered in the partner list without a name are not permitted.

DYNAMIC-PARTNERS = *ON
Dynamic partners are permitted. This means that transfer requests are also permitted with partner systems which are not entered in the partner list or only have their address entered there.

ADM-PORT =
This option allows you to specify the port number used for remote administration.
Default setting following installation: 11000

ADM-PORT = <u>*UNCHANGED</u>
The previous value is unchanged**.**

ADM-PORT = *STD
The port number is set to the default value 11000.

ADM-PORT = <integer 1..65535>
Specifies a valid port number.

ACTIVE-APPLICATIONS=
This option allows you to activate or deactivate the asynchronous inbound server.
Default setting following installation: *OPENFT,*ADM

ACTIVE-APPLICATIONS = <u>*UNCHANGED</u>
The previous value is unchanged**.**

ACTIVE-APPLICATIONS = *ALL
The asynchronous inbound servers for the openFT, ADM and FTP protocols are activated.

ACTIVE-APPLICATIONS = *NONE
The asynchronous inbound servers for the openFT, ADM and FTP protocols are deactivated.

ACTIVE-APPLICATIONS = list-poss(3): *OPENFT / *ADM / *FTP
You can activate the asynchronous inbound servers for specific protocols (openFT, ADM, and/or FTP), by specifying a comma-delimited list of one or more asynchronous inbound servers listed.
The asynchronous inbound servers for the protocol types that are not in the list are then automatically deactivated.

ACTIVE-APPLICATIONS = *OPENFT
Activates the asynchronous inbound server for requests via the openFT protocol.

ACTIVE-APPLICATIONS = *ADM
Activates the asynchronous inbound server for administration requests.

ACTIVE-APPLICATIONS = *FTP
Activates the asynchronous inbound server for requests via the FTP protocol.

ADM-CONNECTION-LIMIT =
This allows you to specify the maximum number of connections for remote administration.
Default setting following installation: 8

ADM-CONNECTION-LIMIT = <u>*UNCHANGED</u>
The previous value is unchanged.

ADM-CONNECTION-LIMIT = <integer 1..255>
You can enter a value between 1 and 255 here.
The default value after installation is 8.

MONITORING =
Activates or deactivates the monitoring functions.
Default setting following installation: *OFF

MONITORING = <u>*UNCHANGED</u>
The monitoring settings remain unchanged.

MONITORING = *ON
Activates monitoring without changing the filter.

MONITORING = *OFF
Deactivates monitoring.

MONITORING = *PARAMETERS(...)
Selects the options that are to be applied to monitoring.

SWITCH =
Activates or deactivates monitoring for the selected partners.
Default setting following installation: *OFF

SWITCH = *UNCHANGED
The previous value is unchanged.

SWITCH = *ON
Activates monitoring.

SWITCH = *OFF
Deactivates monitoring.

PARTNER-SELECTION =
Selects the partners that are to be monitored.
Default setting following installation: *ALL

PARTNER-SELECTION = *UNCHANGED
The previous value is unchanged.

PARTNER-SELECTION = *ALL
All the partners are selected for monitoring.

PARTNER-SELECTION = *NONE
No partner is selected for monitoring. In this event, only certain monitoring data values are populated, see the section “Description of the monitoring values” on page 343.

PARTNER-SELECTION = *OPENFT
All partners which are addressed via the openFT protocol are selected for monitoring.

PARTNER-SELECTION = *FTAM
All partners which are addressed via the FTAM protocol are selected for monitoring.

PARTNER-SELECTION = *FTP
All partners which are addressed via the FTP protocol are selected for monitoring.

REQUEST-SELECTION =
Selects the request types for which monitoring data is to be collected.
Default setting following installation: *ALL

REQUEST-SELECTION = *UNCHANGED
The previous value is unchanged.

REQUEST-SELECTION = *ALL
All requests are selected for monitoring.

REQUEST-SELECTION = *ONLY-SYNC
All synchronous requests are selected for monitoring. Synchronous requests are always issued locally.

REQUEST-SELECTION = *ONLY-ASYNC
All asynchronous requests are selected for monitoring. Requests issued remotely are always regarded as asynchronous.

REQUEST-SELECTION = *ONLY-LOCAL
All locally submitted requests are selected for monitoring.

REQUEST-SELECTION = *ONLY-REMOTE
All remotely submitted requests are selected for monitoring.

ADM-TRAPS =
Specifies the settings for the ADM trap server and the ADM traps.
Default setting following installation: *NONE

ADM-TRAPS = <u>*UNCHANGED</u>
The previous settings remain unchanged.

ADM-TRAPS = *NONE
The ADM trap server is removed from the list, the FTAC transfer admission is deleted and all ADM traps are deactivated.

ADM-TRAPS = *PARAMETERS(...)
Changes the name of the destination, i.e. the ADM trap server and the associated FTAC transfer admission and activates or deactivates selected ADM traps.

DESTINATION =
Here you specify the name of the destination or the ADM trap server together with the corresponding FTAC transfer admission.
Default setting following installation: *NONE

DESTINATION = <u>*UNCHANGED</u>
The name of the ADM trap server and the FTAC transfer admission remain unchanged.

DESTINATION = *NONE
The name of the ADM trap server and the FTAC transfer admission are deleted and thus reset to *NONE.

DESTINATION = *PARAMETERS(...)
Destination to which the ADM traps are to be sent.

PARTNER = <u>*UNCHANGED</u>
The name of the ADM trap server remains unchanged.

PARTNER = <text 1..200 with-low>
Name of the partner system from the partner list or the address of the partner system to which the ADM traps are to be sent. If the partner is not entered in the partner list, it must be specified with the prefix ftadm://, see section "Defining partner properties" on page 44.

TRANSFER-ADMISSION =
FTAC transfer admission for accessing the ADM trap server.

TRANSFER-ADMISSION = *UNCHANGED
The FTAC transfer admission of the ADM trap server remains unchanged.

TRANSFER-ADMISSION = <alphanum-name 8..32> / < c-string 8..32 with-low> / <x-string15..64>
The FTAC functionality is used on the remote system. Only the transfer admission defined in the admission profile may be used.

TRANSFER-ADMISSION = *SECRET
The system prompts you to input the transfer admission. However, this is not visible on the screen.

SELECTION =
Activates or deactivates specific ADM traps.
Default setting following installation: *NONE

SELECTION = *UNCHANGED
The previous value is unchanged.

SELECTION = *NONE
Deactivates all ADM traps.

SELECTION = *ALL
Activates all ADM traps.

SELECTION = *PARAMETERS(...)
Activates or deactivates selected ADM traps.

FT-STATE =
Activates or deactivates the sending of traps on START-FT / STOP-FT and if openFT is terminated abnormally.
Default setting following installation: *OFF

FT-STATE = *UNCHANGED
The previous value is unchanged.

FT-STATE = *OFF
Deactivates the traps for FT-STATE.

FT-STATE = *ON
Activates the traps for FT-STATE.

PARTNER-STATE =
Activates or deactivates the sending of traps when the status of partners changes.
Default setting following installation: *OFF

PARTNER-STATE = *UNCHANGED
The previous value is unchanged.

PARTNER-STATE = *OFF
Deactivates the traps for PARTNER-STATE.

PARTNER-STATE = *ON
Activates the traps for PARTNER-STATE.

PARTNER-UNREACHABLE =
Activates or deactivates the sending of the trap indicating that a partner is unreachable.
Default setting following installation: *OFF

PARTNER-UNREACHABLE = *UNCHANGED
The previous value is unchanged.

PARTNER-UNREACHABLE = *OFF
Deactivates the "partner unreachable" trap.

PARTNER-UNREACHABLE = *ON
Activates the "partner unreachable" trap.

REQUEST-QUEUE-STATE =
Activates the sending of traps referring to the filling level of the request queue, i.e. whether traps are sent if the filling level has exceeded the 85% threshold or fallen below the 80% threshold.
Default setting following installation: *OFF

REQUEST-QUEUE-STATE = *UNCHANGED
The previous value is unchanged.

REQUEST-QUEUE-STATE = *OFF
Deactivates the traps if the filling level falls outside the thresholds.

REQUEST-QUEUE-STATE = *ON
Activates the traps if the filling level falls outside the thresholds.

TRANSFER-SUCCESS =
Activates or deactivates the sending of the trap indicating that an FT request was completed successfully.
Default setting following installation: *OFF

TRANSFER-SUCCESS = *UNCHANGED
The previous value is unchanged.

TRANSFER-SUCCESS = *OFF
Deactivates the trap for TRANSFER-SUCCESS.

TRANSFER-SUCCESS = *ON
Activates the trap for TRANSFER-SUCCESS.

TRANSFER-FAILURE =
Activates or deactivates the sending of the trap indicating that an FT request was aborted.
Default setting following installation: *OFF

TRANSFER-FAILURE = <u>*UNCHANGED</u>
The previous value is unchanged.

TRANSFER-FAILURE = *OFF
Deactivates the trap for TRANSFER-FAILURE.

TRANSFER-FAILURE = *ON
Activates the trap for TRANSFER-FAILURE.

ENCRYPTION-MANDATORY =
Controls the system-wide obligation for user data encryption. This setting applies for transfer and administration requests.
Default setting following installation: *NO

ENCRYPTION-MANDATORY = <u>*UNCHANGED</u>
The setting remains unchanged.

ENCRYPTION-MANDATORY = *NO
Deactivates the system-wide obligation for user data encryption. If encryption is required, this must be specified explicitly in the request.

ENCRYPTION-MANDATORY = *INBOUND
Activates the obligation for inbound encryption:
Inbound requests must transfer the user data in encrypted form, otherwise they are rejected.

ENCRYPTION-MANDATORY = *OUTBOUND
Activates the obligation for outbound encryption, i.e.:
Outbound requests transfer the user data in encrypted form, even if no encryption was called for in the request (e.g. TRANSFER-FILE, program interface, etc.).

ENCRYPTION-MANDATORY = (*INBOUND,*OUTBOUND)
Activates the obligation for inbound and outbound encryption, i.e:
Inbound requests must be transferred in encrypted form, otherwise they are rejected. Outbound requests transfer the user data in encrypted form, even if no encryption was called for in the request.

- System-wide mandatory encryption may be activated only if openFT-CR is installed. Deactivation with ENCRYPTION-MANDATORY=*NO is, on the other hand, permitted even if openFT-CR is no (longer) installed.
- When mandatory inbound encryption is activated, inbound FTAM requests and inbound FTP requests are rejected.
  When mandatory outbound encryption is activated, outbound FTAM requests are rejected. Outbound FTP requests are, however, permitted.
- File management requests are executed in unencrypted format irrespective of the specification in ENCRYPTION-MANDATORY.

DELETE-LOGGING =
Controls the settings for deleting log records.

DELETE-LOGGING = *UNCHANGED
The settings for deleting log records remain unchanged.

DELETE-LOGGING = *PARAMETERS(...)
Defines the options for deleting log records.

SWITCH =
Activates or deactivates the automatic deletion of log records.
Default setting following installation: *OFF

SWITCH = *UNCHANGED
The automatic deletion of log records remains activated or deactivated.

SWITCH = *ON
Activates the automatic deletion of log records.

SWITCH = *OFF
Deactivates the automatic deletion of log records.

RETENTION-PERIOD =
Specifies the minimum age of the log records for deletion.
Default setting following installation: 14 days.

RETENTION-PERIOD = *UNCHANGED
The settings remain unchanged.

RETENTION-PERIOD = <integer 0..999 days>
Minimum age of log records for deletion in days. The days are counted back from the deletion time specified in DELETE-TIME. The value 0 deletes all the log records that were written before or at the time of the current day specified in DELETE-TIME.

REPEAT =
Specifies when deletion is to be repeated.
Default setting following installation: *DAILY

REPEAT = *UNCHANGED
The settings remain unchanged.

REPEAT = *DAILY
The log records are deleted every day.

REPEAT = *WEEKLY(..)
The log records are deleted once a week.

ON = *SUNDAY / *MONDAY / *TUESDAY / *WEDNESDAY / *THURSDAY / *FRIDAY / *SATURDAY
Weekday on which the log records are deleted.

REPEAT = *MONTHLY(..)
The log records are deleted once a month.

ON = 1 / <integer 1..31>
Specific day of the month (1-31). If 29, 30 or 31 is specified as the day of the month but the month has fewer days, deletion will take place on the last day of the month.

DELETE-TIME =
Specifies the time at which the log records are to be deleted.
Default setting following installation: 00:00

DELETE-TIME = *UNCHANGED
The setting remains unchanged.

DELETE-TIME = <time 1..8>
Time (local time at which the log records are to be deleted. Due to the nature of the system, the delete function can be performed up to 5 minutes after this time. You enter the time in the format *hh:mm:ss*, e.g. 14:30:10.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
87	32	CMD0221	No space left on device for internal files.
33	64	FTR1033	The public key files could not be updated.
35	64	FTR1035	Command only permissible for FT administrator.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

The maximum number of tasks to be executed in parallel is to be 3 and the maximum number of transport connections to be set up is to be 10:

```
/MODIFY-FT-OPTIONS PROCESS-LIMIT=3,CONNECTION-LIMIT=10
```

5.25 MODIFY-FT-PARTNER Modify partner properties in the partner list

Note on usage

User group: FT administrator

Alias name: FTMODPTN

Functional description

This command can be used to modify the characteristics of a partner that is already entered in the partner list. When changing the partner address, please note that an openFT partner cannot be changed to an FTP partner or an FTAM partner and vice versa.

You can remove an entered dynamic partner from the partner list by setting all the properties to the default values for free dynamic partners by means of the MODIFY-FT-PARTNER command. The default values are the same as the default values in the ADD-FT-PARTNER command with the exception of the SECURITY-LEVEL operand which must be set to *BY-PARTNER-ATTRIBUTES.

Similarly, you can add a free dynamic partner to the partner list by setting at least one of its attributes to a value other than the default. This is possible if PARTNER does not reference a partner list entry and PARTNER-ADDRESS is not specified.

If a partner name for which there is as yet no partner list entry is specified for PARTNER and PARTNER-ADDRESS is also specified, a new named partner list entry is created. This function is intended for the re-import of exported partner entries. To explicitly create new partner entries, you should use ADD-FT-PARTNER .

Format

```
MODIFY-FT-PARTNER / FTMODPTN

 PARTNER = *ALL / <text 1..200 with-low>
,STATE = *UNCHANGED / *PARAMETERS(...)
    *PARAMETERS(...)
        OUTBOUND = *UNCHANGED / *ACTIVE(...) / *DEACT
            *ACTIVE(...)
                AUTOMATIC-DEACT = *NO / *YES
        ,INBOUND = *UNCHANGED / *ACTIVE / *DEACT
,SECURITY-LEVEL = *UNCHANGED / *STD / *BY-PARTNER-ATTRIBUTES / <integer 1..100>
,PARTNER-ADDRESS = *UNCHANGED / <text 1..200 with-low>
,TRACE = *UNCHANGED / *BY-FT-OPTIONS / *ON / *OFF
,IDENTIFICATION = *UNCHANGED / *STD / <composed-name 1..64> / <c-string 1..64 with-low>
,SESSION-ROUTING-INFO = *UNCHANGED / *NONE / *IDENTIFICATION / <alphanum-name 1..8>
,PARTNER-CHECK = *UNCHANGED / *BY-FT-OPTIONS / *STD / *TRANSPORT-ADDRESS
,AUTH-MANDATORY = *UNCHANGED / *NO / *YES
,PRIORITY= *UNCHANGED / *NORMAL / *LOW / *HIGH
,REQUEST-PROCESSING = *UNCHANGED / *STD / *SERIAL
```

Operands

PARTNER =
Specifies the partner system.

PARTNER = *ALL
The specified changes are to be implemented for all partner systems defined in the partner list. This specification is only meaningful in conjunction with the operands STATE, SECURITY-LEVEL, TRACE , PARTNER-CHECK, AUTH-MANDATORY, PRIORITY and REQUEST-PROCESSING.

Particular care is necessary when using PARTNER=*ALL in combination with the SECURITY-LEVEL operand.

> The description below refers to a single partner system. If you have selected *ALL, the description applies by analogy for all partner system in the partner list which comply with the relevant selection criteria.

PARTNER = <text 1..200 with-low>
Specifies either the name of the partner system from the partner list or the address of the partner system (see section “Defining partner properties” on page 44).

STATE =
Controls the state of the partner system (activated, deactivated).

STATE = *UNCHANGED
The state is unchanged.

STATE = *PARAMETERS(...)
Specifies the settings for locally submitted file transfer requests (outbound) and for remotely submitted file transfer requests.

OUTBOUND =
Specifies the setting for locally submitted file transfer requests to the partner system.

OUTBOUND = *UNCHANGED
The state of locally submitted FT requests is unchanged.

OUTBOUND = *ACTIVE(...)
Locally submitted file transfer requests to the partner system are processed.

AUTOMATIC-DEACT =
Defines if repeated attempts to establish a connection with this partner system should result in a deactivation of the partner system after multiple attempts.

AUTOMATIC-DEACT = *NO
Unsuccessful attempts to establish a connection with this partner system do not lead to its deactivation.

AUTOMATIC-DEACT = *YES
Repeated unsuccessful attempts to establish a connection with this partner system lead to its deactivation. If locally submitted files transfer requests to the partner system are to be executed again after this, the system must be activated explicitly (with OUTBOUND=*ACTIVE).

OUTBOUND = *DEACT
Locally submitted file transfer requests to the partner system are initially not processed (not started) but are stored in the request queue. They are executed only after the partner system has been activated with OUTBOUND=*ACTIVE.

INBOUND =
Specifies the setting for remotely submitted file transfer requests, i.e. requests which were submitted by this partner system.

INBOUND = *UNCHANGED
The state of locally submitted FT requests is unchanged.

INBOUND = *ACTIVE
Remotely submitted file transfer requests from this partner system are processed.

INBOUND = *DEACT
Remotely submitted synchronous file transfer requests from this partner system are rejected. Remotely submitted asynchronous file transfer requests from this partner system are stored there and cannot be processed until the partner system is activated again with INBOUND=*ACTIVE.

SECURITY-LEVEL =
Assigns a security level to a remote system.

SECURITY-LEVEL = *UNCHANGED
The value is unchanged.

SECURITY-LEVEL = *STD
If you set this operand to *STD, a standard security level is assigned to the remote system. This standard security level is defined using the MODIFY-FT-OPTIONS command. Here you can define a fixed value or make the value attribute-dependent.

SECURITY-LEVEL = *BY-PARTNER-ATTRIBUTES
If you set the operand to *BY-PARTNER-ATTRIBUTES then the security level is defined automatically:

– Partners that are authenticated by openFT are assigned the security level 10.
– Partners, that are known in BCAM (i.e. they are addressed via their BCAM names), are assigned the security level 90.
– All other partners are assigned security level 100.

SECURITY-LEVEL = <integer 1..100>
Must be specified if you want to assign a particular security level to the individual partner system.

PARTNER-ADDRESS =
Address of the partner system.

PARTNER-ADDRESS = *UNCHANGED
The address remains unchanged.

PARTNER-ADDRESS = <text 1..200 with-low>
New address for the partner system. For details on the address format, see section “Defining partner properties” on page 44.

TRACE =
Trace setting for the partner systems. Trace entries are generated only if the FT trace function is activated by means of an operating parameter (MODIFY-FT-OPTIONS TRACE=*ON).

TRACE = *UNCHANGED
The current trace setting is unchanged.

TRACE = *BY-FT-OPTIONS
The trace settings specified in the MODIFY-FT-OPTIONS command are used.

TRACE = *ON
Activates the trace for this partner system even if tracing is deactivated for this partner type in the global settings (MODIFY-FT-OPTIONS). The request-specific trace settings made in MODIFY-FT-OPTIONS, on the other hand, are taken into account.

i A detailed description of the trace function can be found in section “Diagnostics” on page 91.

TRACE = *OFF
For connections to this partner system, only those trace entries which it is technically impossible to suppress are generated. Trace entries which it is technically impossible to suppress are those which are generated before openFT (BS2000) identifies the partner system

IDENTIFICATION =
The network-wide, unique ID of the openFT instance in the partner system.

IDENTIFICATION = *UNCHANGED
The ID remains unchanged.

IDENTIFICATION = *STD
For openFT and FTADM partners, the partner address or the host name from the partner address is used as the identification. No identification is set for FTP and FTAM partners.

IDENTIFICATION = <composed-name 1..64> / <c-string 1..64 with-low>
The network-wide, unique instance ID of the openFT instance in the partner system. This ID is used for authenticating partner systems as of openFT V8.1. It is set by the FT administrator of the partner system (in BS2000, by using MODIFY-FT-OPTIONS IDENTIFICATION=, in Unix systems or Windows, by using *ftmodo -id*). The uniqueness of this ID must be based on something other than case-sensitivity. An instance ID may be comprised of alphanumeric characters or special characters. It is advisable to use only the special characters “.”, “-”, “:” or “%”.

The initial character must be alphanumeric or the special character “%”. The “%” character may only be used as an initial character. An alphanumeric character must follow the “.” character. For more details on assigning instance identifications, see page 55.

With FTAM partners an Application Entity Title can be specified as an identification in the format *n1.n2.n3.n4..mmm*. For details, see the section "Addressing via Application Entity Title" in the openFT User Guide.

The instance identification must not be specified with FTP partners!

i You should always specify the instance identification of the partner system explicitly (except with FTAM or FTP partners) and should not use the default value (IDENTIFICATION=*STD).

SESSION-ROUTING-INFO =
If the partner system is only accessible via a go-between instance, specify here the address information, which the go-between instance will use for re-routing. This is necessary, for example, for partner systems using openFT for OS/390 and z/OS, dependent on TRANSIT coupling.

SESSION-ROUTING-INFO = *UNCHANGED
The setting remains unchanged.

SESSION-ROUTING-INFO = *NONE
No routing information is used. The session selector can be specified as part of the partner address.

SESSION-ROUTING-INFO = *IDENTIFICATION
Connections to the partner are re-routed via a gateway that uses the instance identification as the address information.

SESSION-ROUTING-INFO = <alphanum-name 1..8>

PARTNER-CHECK =
Enables the global settings for sender checking to be modified on a partner-specific basis. These settings are only effective for named openFT partners that do not work with authentication (see section “Authentication” on page 53).

This setting has no meaning for FTAM partners, FTP partners and dynamic partner entries.

PARTNER-CHECK = *UNCHANGED
The set value remains unchanged.

PARTNER-CHECK = *BY-FT-OPTIONS
The global settings are valid for the partner.

PARTNER-CHECK = *STD
Disable the expanded sender checking. The transport address of the partner is not checked, even if the expanded sender checking is globally enabled (see the MODIFY-FT-OPTIONS command).

PARTNER-CHECK = *TRANSPORT-ADDRESS
Enables expanded sender checking. The transport address is checked, even if the expanded sender checking is globally disabled (see the MODIFY-FT-OPTIONS command). If the transport address under which the partner is reporting does not correspond to the entry in the partner list, the request is rejected.

AUTH-MANDATORY =
Forces the authentication of a named partner system.

AUTH-MANDATORY = *UNCHANGED
The set value is unchanged.

AUTH-MANDATORY = *NO
Authentication is not forced, i.e. this partner system is not restricted with regard to authentication.

AUTH-MANDATORY = *YES
Authentication is forced, i.e. connections to and from this named partner are only permitted when authentication is provided.

PRIORITY=
This operand allows you to specify the priority of the partner system in respect of processing requests that have the same request priority. This means that the partner priority only applies in the case of requests that have the same request priority, but that are issued to partners with a different partner priority.

PRIORITY = *<u>*UNCHANGED</u>*
The priority of the partner system with regard to the processing of requests with the same request priority remains unchanged.

PRIORITY = <u>*NORMAL</u>
The partner has normal priority.

PRIORITY = *LOW
The partner has low priority.

PRIORITY = *HIGH
The partner has high priority.

REQUEST-PROCESSING =
You use this option to control whether asynchronous outbound requests to this partner system are always run serially or whether parallel connections are permitted.

REQUEST-PROCESSING = <u>*UNCHANGED</u>
The operating mode to this partner system remains unchanged.

REQUEST-PROCESSING = *STD
Parallel connections to this partner system are permitted.

REQUEST-PROCESSING = *SERIAL
Parallel connections to this partner system are not permitted. If multiple file transfer requests to this partner system are pending, then they are processed serially. A follow-up request is consequently not started until the preceding request has terminated.

Command return codes

(SC2)	SC1	Maincode	Meaning
198	1	CMD0202	Invalid parameter value.
83	32	CMD0221	Internal error.
35	64	FTR1035	Command only permissible for FT administrator.
43	64	FTR1043	Partner with same attribute already exists in partner list.
44	64	FTR1044	Maximum number of partners exceeded.
45	64	FTR1045	Partner name not found in partner list.
46	64	FTR1046	Modification of partner protocol type not possible.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example 1

The SECURITY-LEVEL for the partner system TEST is set to 99:

```
/MODIFY-FT-PARTNER PARTNER=TEST,SECURITY-LEVEL=99
```

Example 2

The port number for partner WINDOWS (host name = winhost2) is set to 1100:

```
/MODIFY-FT-PARTNER PARTNER=WINDOWS,PARTNER-ADDRESS=winhost2:1100
```

5.26 MODIFY-FT-PROFILE Modify admission profile

User instruction

User group: FTAC user and FTAC administrator

Prerequisite for using this command is the use of openFT-AC.

Functional description

The command MODIFY-FT-PROFILE can be used by any FTAC user to modify his/her admission profile. In a privileged admission profile, an FTAC user can only modify the operands TRANSFER-ADMISSION and PRIVILEGED.

When the FTAC administrator neither possesses TSOS privilege nor has specified the account number and password, the profile is prohibited after a modification and must be released by the user. Modification of the privilege is excluded from this: in this case the profile is not locked.

As soon as an admission profile is modified, the timestamp of the last modification is also updated. You can see the timestamp with SHOW-FT-PROFILE INF=*ALL (LAST-MODIF). The timestamp is also updated if you do not change the properties of the profile, i.e. if you enter MODIFY-FT-PROFILE with the parameter NAME without specifying other parameters.

Format

(part 1 of 3)

```
MODIFY-FT-PROFILE

 NAME = *ALL / *STD / <alphanum-name 1..8>
,PASSWORD = *NONE / <c-string 1..8 with-low> / <x-string 1..16> / *SECRET
,SELECT-PARAMETER = *OWN / *PARAMETERS(...)
  *PARAMETERS(...)
   |  TRANSFER-ADMISSION = *ALL / *NOT-SPECIFIED / <alphanum-name 8..32> /
   |                       c-string 8..32 with-low> / <x-string 15..64> / *SECRET
   | ,OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
,NEW-NAME = *OLD / *STD / <alphanum-name 1..8>
,TRANSFER-ADMISSION = *UNCHANGED / *NOT-SPECIFIED / *OLD-ADMISSION(...) /
                      <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...) /
                      *SECRET
  *OLD-ADMISSION(...)
   |  VALID = *UNCHANGED / *YES / *NO
   | ,USAGE = *UNCHANGED / *PRIVATE / *PUBLIC
   | ,EXPIRATION-DATE = *UNCHANGED / *NOT-RESTRICTED / <date 8..10>
  <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...)
   |  VALID = *YES / *NO / *UNCHANGED
   | ,USAGE = *PRIVATE / *PUBLIC / *UNCHANGED
   | ,EXPIRATION-DATE = *NOT-RESTRICTED / <date 8..10> / *UNCHANGED
,PRIVILEGED = *UNCHANGED / *NO / *YES
,IGNORE-MAX-LEVELS = *UNCHANGED / *NO / *YES / *PARAMETERS(...)
  *PARAMETERS(...)
   |  OUTBOUND-SEND = *UNCHANGED / *NO / *YES
   | ,OUTBOUND-RECEIVE = *UNCHANGED / *NO / *YES
   | ,INBOUND-SEND = *UNCHANGED / *NO / *YES
   | ,INBOUND-RECEIVE = *UNCHANGED / *NO / *YES
   | ,INBOUND-PROCESSING = *UNCHANGED / *NO / *YES
   | ,INBOUND-MANAGEMENT = *UNCHANGED / *NO / *YES
```

(part 2 of 3)

```
,USER-ADMISSION = *UNCHANGED / *OWN / *PARAMETERS(...)
   *PARAMETERS(...)
        USER-IDENTIFICATION = *OWN / <name 1..8>
       ,ACCOUNT = *OWN / *FIRST / *NOT-SPECIFIED / *NONE / <alphanum-name 1..8>
       ,PASSWORD = *OWN / *NOT-SPECIFIED / <c-string 1..8> / <c-string 9..32> / <x-string 1..16> /
                   *NONE / *SECRET
,INITIATOR = *UNCHANGED / list-poss(2): *REMOTE / *LOCAL
,TRANSFER-DIRECTION = *UNCHANGED / *NOT-RESTRICTED / *FROM-PARTNER / *TO-PARTNER
,PARTNER = *UNCHANGED / *NOT-RESTRICTED / *ADD(...) / *REMOVE(...) /
           list-poss(50): <text 1..200 with-low>
   *ADD(...)
        NAME = list-poss(50): <text 1..200 with-low>
   *REMOVE(...)
        NAME = list-poss(50): <text 1..200 with-low>
,MAX-PARTNER-LEVEL = *UNCHANGED / *NOT-RESTRICTED / <integer 0..100>
,FILE-NAME = *UNCHANGED / *NOT-RESTRICTED  / <filename1..54 > /
             <c-string 1..512 with-low> /  *EXPANSION(...) / *LIBRARY-ELEMENT(...) /
             *POSIX(NAME=<posix-pathname 1..510>)
   *EXPANSION(...)
        PREFIX = <filename 1..53> / <partial-filename 2..53> / <c-string 1..511 with-low>
   *LIBRARY-ELEMENT(...)
        LIBRARY = *UNCHANGED / *NOT-RESTRICTED / <filename 1..54> / *EXPANSION(...)
           *EXPANSION(...)
                PREFIX = <filename 1..53> / <partial-filename 2..53>
       ,ELEMENT = *UNCHANGED / *NOT-RESTRICTED /
                  <composed-name 1..64 with-under>(...) / *EXPANSION(...)
            <composed-name 1..64 with-under>(...)
                VERSION = *STD / <text 1..24>
           *EXPANSION(...)
                PREFIX = <composed-name 1..63 with-under> / <partial-filename 2..63>
       ,TYPE = *UNCHANGED / *NOT-RESTRICTED / <name 1..8>
,FILE-PASSWORD = *UNCHANGED / *NOT-RESTRICTED / *NONE / <c-string 1..4> /
                 <x-string 1..8> / <integer -2147483648...2147483647> / *SECRET
```

(part 3 of 3)

```
,PROCESSING-ADMISSION = *UNCHANGED / *SAME / *NOT-RESTRICTED / *PARAMETERS(...)

   *PARAMETERS(...)
     |  USER-IDENTIFICATION = *SAME / *NOT-RESTRICTED / <name 1..8>
     | ,ACCOUNT = *SAME / *NOT-RESTRICTED / *NONE / <alphanum-name 1..8>
     | ,PASSWORD = *SAME / *NOT-RESTRICTED / *NONE / <c-string 1..8> / <c-string 9..32> /
     |                <x-string 1..16> / *SECRET

,SUCCESS-PROCESSING = *UNCHANGED / *NOT-RESTRICTED / *NONE / <c-string 1..1000 with-low> /
                      *EXPANSION(...)

   *EXPANSION(...)
     |  PREFIX = *UNCHANGED / *NOT-RESTRICTED / <c-string 1..999 with-low>
     | ,SUFFIX = *UNCHANGED / *NOT-RESTRICTED / <c-string 1..999 with-low>

,FAILURE-PROCESSING = *UNCHANGED / *NOT-RESTRICTED / *NONE / <c-string 1..1000 with-low> /
                      *EXPANSION(...)

   *EXPANSION(...)
     |  PREFIX = *UNCHANGED / *NOT-RESTRICTED / <c-string 1..999 with-low>
     | ,SUFFIX = *UNCHANGED / *NOT-RESTRICTED / <c-string 1..999 with-low>

,WRITE-MODE = *UNCHANGED / *NOT-RESTRICTED / *NEW-FILE / *REPLACE-FILE / *EXTEND-FILE

,FT-FUNCTION = *UNCHANGED / *NOT-RESTRICTED / list-poss(5):
               *TRANSFER-FILE / *MODIFY-FILE-ATTRIBUTES / *READ-DIRECTORY /
               *FILE-PROCESSING / *REMOTE-ADMINISTRATION

,USER-INFORMATION = *UNCHANGED / *NONE / <c-string 1..100 with-low>

,DATA-ENCRYPTION = *UNCHANGED / *NOT-RESTRICTED / *NO / *YES
```

Operands

NAME =
Determines the name of the admission profile to be modified.

NAME = *ALL
Modifies all admission profiles at the same time provided no further selection criteria are specified using the SELECT parameter and neither the name nor the transfer admission is to be modified.

NAME = *STD
Changes the default admission profile for your user ID or, as FTAC administrator, the default authorization profile of the selected user ID.

NAME = <alphanum-name 1..8>
Modifies the admission profile with this name.

PASSWORD =
FTAC password which authorizes you to use FTAC commands on your user ID, if such a password has been defined in your admission set.

PASSWORD = *NONE
No FTAC password is required.

PASSWORD = <c-string 1..8 with-low> / <x-string 1..16>
This FTAC password is required.

PASSWORD = *SECRET
The system prompts you to enter the password. However, it does not appear on the screen.

SELECT-PARAMETER =
Specifies a transfer admission. You will then modify the admission profile which has this transfer admission.

SELECT-PARAMETER = *OWN
Modifies your own admission profile.

SELECT-PARAMETER = *PARAMETERS(...)
Specifies the selection criteria for the profiles which you wish to modify.

TRANSFER-ADMISSION =
Entering the TRANSFER-ADMISSION here makes it a selection criterion for the admission profiles which you wish to modify.

TRANSFER-ADMISSION = *ALL
All your admission profiles are to be modified, irrespective of the transfer admission.

TRANSFER-ADMISSION = *NOT-SPECIFIED
Only admission profiles without a defined transfer admission are to be modified. In the case of a default admission profile, the transfer admission is never assigned, because this is addressed using the user ID and the user password.

TRANSFER-ADMISSION = <alphanum-name 8..32> / <c-string 8..32 with-low> / <x-string 15..64>
The admission profile with this transfer admission is to be modified.

TRANSFER-ADMISSION = *SECRET
The system prompts you to enter the transfer admission. However, it does not appear on the screen.

OWNER-IDENTIFICATION =
You can use the owner of an admission profile as a selection criterion for access to a profile to be modified.

OWNER-IDENTIFICATION = *OWN
Modifies your own admission profile.

OWNER-IDENTIFICATION = *ALL
The FTAC administrator can access the profiles of all users. The FTAC user is not permitted to make this entry.

OWNER-IDENTIFICATION = <name 1..8>
The FTAC user can enter only his/her own user ID here, the FTAC administrator can enter any user ID.

NEW-NAME =
NEW-NAME is used to assign a new name to the admission profile.
NEW-NAME may only be specified together with unambiguous selection criteria (NAME or TRANSFER-ADMISSION).

NEW-NAME = *OLD
The name of the admission profile remains unchanged.

NEW-NAME = *STD
Makes the admission profile the default admission profile for the user ID. If the admission profile previously had a transfer admission, you must also specify TRANSFER-ADMISSION=*NOT-SPECIFIED.

NEW-NAME = <alphanum-name 1..8>
New name of the admission profile. This name must be unique among all the admission profiles on your user ID. If an admission profile with this name already exists, FTAC rejects the command with the following message:

```
FTC0100   FT profile already exists
```

The command SHOW-FT-PROFILE (see page 372ff) can be used to obtain information on the already existing name. For this information, it suffices to enter SHOW-FT-PROFILE without parameters.

TRANSFER-ADMISSION =
Modifies the transfer admission which is associated with the admission profile selected. You must ensure that the transfer admission is unique within your openFT system. If the transfer admission which you have selected already exists, FTAC rejects the command with the following message:

```
FTC0101   Transfer admission already exists
```

The FTAC administrator can also allocate an transfer admission here if he/she modifies the admissions profile of any user ID. If he/she has no TSOS privilege, the FTAC administrator must also specify the complete USER-ADMISSION for the affected user ID (USER-IDENTIFICATION, ACCOUNT, and PASSWORD).
TRANSFER-ADMISSION may only be specified together with unambiguous selection criteria (NAME or SELECT-PARAMETERS=*PAR(TRANSFER-ADMISSION).

TRANSFER-ADMISSION = *UNCHANGED
The transfer admission remains unchanged.

TRANSFER-ADMISSION = *NOT-SPECIFIED
No transfer admission is set and any existing transfer admissions are made invalid. This blocks the profile, provided that it is not a profile that you are converting to a default admission profile. In this case, you must specify *NOT-SPECIFIED.

TRANSFER-ADMISSION = *OLD-ADMISSION(...)
The transfer admission itself remains unchanged. The options, however, can be changed, as opposed to with the entry TRANSFER-ADMISSION=*UNCHANGED. The specifications are ignored if you are changing a default admission profile.

VALID = <u>*UNCHANGED</u>
The value remains unchanged.

VALID = *YES
The transfer admission is valid.

VALID = *NO
The transfer admission is not valid. The profile can be blocked with this entry.

USAGE = <u>*UNCHANGED</u>
The value remains unchanged.

USAGE = *PRIVATE
Access to your profile is denied for security reasons whenever another user ID attempts to set for a second time the TRANSFER-ADMISSION which has already been used by you.

USAGE = *PUBLIC
Access to your profile is not denied if another user happens to “discover” your TRANSFER-ADMISSION. “Discovery” means that another user ID attempted to specify the same TRANSFER ADMISSION twice. This is rejected for uniqueness reasons.

EXPIRATION-DATE = <u>*UNCHANGED</u>
The value remains unchanged.

EXPIRATION-DATE = *NOT-RESTRICTED
The use of this transfer admission is not restricted with respect to time.

EXPIRATION-DATE = <date 8..10>
Date in the form *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2013-03-31 or 13-03-31 for 31 March, 2013.The use of the transfer admission is only possible until the given date.

TRANSFER-ADMISSION = <alphanum-name 8..32>(...) / <c-string 8..32 with-low>(...) / <x-string 15..64>(...)
The character string must be entered as transfer admission in the transfer request. The alphanumeric input is always stored in lowercase letters.

VALID = <u>*YES</u>
The transfer admission is valid.

VALID = *NO
The transfer admission is not valid. The profile can be blocked with this entry.

VALID = *UNCHANGED
The value remains unchanged.

USAGE = <u>*PRIVATE</u>
Access to your profile is denied for security reasons whenever another user ID attempts to set for a second time the TRANSFER-ADMISSION which has already been used by you.

USAGE = *PUBLIC
Access to your profile is not denied if another user happens to “discover” your TRANSFER-ADMISSION. “Discovery” means that another user ID attempted to specify the same TRANSFER ADMISSION twice. This is rejected for uniqueness reasons.

USAGE = *UNCHANGED
The value remains unchanged.

EXPIRATION-DATE = <u>*NOT-RESTRICTED</u>
The use of this transfer admission is not restricted with respect to time.

EXPIRATION-DATE = <date 8..10>
Date in the form *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2013-03-31 or 13-03-31 for 31 March, 2013.The use of the transfer admission is only possible until the given date.

EXPIRATION-DATE = *UNCHANGED
The value remains unchanged.

TRANSFER-ADMISSION = *SECRET
The system prompts you to input the transfer admission. However, this does not appear on the screen. The operands VALID, USAGE and EXPIRATION-DATE can also be secretly entered in this case.

PRIVILEGED =
The FTAC administrator can privilege the admission profile of any FTAC user. FT requests which are processed with a privileged status are not subject to the restrictions for MAX-ADM-LEVEL in the admission set.
The FTAC user can only reverse any privileged status given.

PRIVILEGED = <u>*UNCHANGED</u>
The status of this admission profile remains unchanged.

PRIVILEGED = *NO
With *NO, you can reverse the privileged status.

PRIVILEGED = *YES
With *YES, the FTAC administrator gives one or more admission profiles privileged status.

IGNORE-MAX-LEVELS =

Determines for which of the six basic functions the restrictions of the admission set should be ignored. The user's MAX-USER-LEVELS can be exceeded in this way. The MAX-ADM-LEVELS in the admission set can only be effectively exceeded with an admission profile which has been designated as privileged by the FTAC administrator. The FTAC user can set up an admission profile for himself/herself for special tasks (e.g. sending a certain file to a partner system with which he/she normally is not allowed to conduct a file transfer), which allows him/her to exceed the admission set. This profile must be explicitly given privileged status by the FTAC administrator.

If you enter IGNORE-MAX-LEVELS=*YES, the settings for all the basic functions are ignored. If you wish to ignore the admission set for specific basic functions, you need to do this with the operands explained later in the text.

The following table shows which partial components of the file management can be used under which conditions:

Inbound file management function	**Setting in admission set/extension in profile**
Show file attributes	Inbound sending (IBS) permitted
Modify file attributes	Inbound receiving (IBR) **and** Inbound file management (IBF) permitted
Rename files	Inbound receiving (IBR) **and** Inbound file management (IBF) permitted
Delete files	Inbound receiving (IBR) permitted **and** write rule = overwrite in profile
Show directories	Inbound file management (IBF) permitted **and** direction = to partner in profile
Create, rename, delete directories	Inbound file management (IBF) permitted **and** direction = from partner in profile

IGNORE-MAX-LEVELS = *UNCHANGED

You can access the same security levels as before the modification (unless you have reversed the privileged status with PRIVILEGED=*NO).

IGNORE-MAX-LEVELS = *NO

FT requests which are processed with the admission profile are subject to the restrictions of the admission set.

IGNORE-MAX-LEVELS = *YES

*YES allows you to communicate with partner systems whose security level exceeds the specifications of the admission set. If your profile does not have privileged status, you can only disregard the MAX-USER-LEVELS in the admission set, not the MAX-ADM-LEVELS. The current MAX-USER-LEVELS and MAX-ADM-LEVELS settings can be accessed using the command SHOW-FT-ADMISSION-SET (see example on page 308).

IGNORE-MAX-LEVELS = *PARAMETERS(...)

OUTBOUND-SEND = *UNCHANGED
The maximum security level which can be reached with the basic function “outbound send” remains unchanged.

OUTBOUND-SEND = *NO
The maximum security level which can be reached with the basic function “outbound send” is determined by the admission set.

OUTBOUND-SEND = *YES
For the basic function “outbound send”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

OUTBOUND-RECEIVE = *UNCHANGED
The maximum security level which can be reached with the basic function “outbound receive” remains unchanged.

OUTBOUND-RECEIVE = *NO
The maximum security level which can be reached with the basic function “outbound receive” is determined by the admission set.

OUTBOUND-RECEIVE = *YES
For the basic function “outbound receive”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

INBOUND-SEND = *UNCHANGED
The maximum security level which can be reached with the basic function “inbound send” remains unchanged.

INBOUND-SEND = *NO
The maximum security level which can be reached with the basic function “inbound send” is determined by the admission set.

INBOUND-SEND = *YES
For the basic function “inbound send”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The same applies to the partial component “display file attributes” of the basic function “inbound file management” can be used.

INBOUND-RECEIVE = *UNCHANGED
The maximum security level which can be reached with the basic function “inbound receive” remains unchanged.

INBOUND-RECEIVE = *NO
The maximum security level which can be reached with the basic function “inbound receive” is determined by the admission set.

INBOUND-RECEIVE = *YES
Disregards your settings for “inbound receive” in the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The same applies to the following partial components of the basic function “inbound file management”:

– delete files, as long as the file attributes are set accordingly,
– modify file attributes, if the basic function “inbound file management” was admitted in the admission set or in the admission profile.

INBOUND-PROCESSING = *UNCHANGED
The maximum security level which can be reached with the basic function “inbound processing” remains unchanged.

INBOUND-PROCESSING = *NO
The maximum security level which can be reached with the basic function “inbound processing” is determined by the admission set.

INBOUND-PROCESSING = *YES
For the basic function “inbound processing”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS.

INBOUND-MANAGEMENT = *UNCHANGED
The maximum security level which can be reached with the basic function “inbound file management” remains unchanged.

INBOUND-MANAGEMENT = *NO
The maximum security level which can be reached with the basic function “inbound file management” is determined by the admission set.

INBOUND-MANAGEMENT = *YES
For the basic function “inbound file management”, you can use this admission profile to disregard the MAX-USER-LEVELS. If your profile is privileged, you are also not held to the restrictions of the MAX-ADM-LEVELS. The partial component “modify file attributes” of the basic function “inbound file management” only functions if the basic function “inbound receive” was admitted in the admission set or admission profile.

USER-ADMISSION =
User ID under which the modified admission profile is saved. FT requests which use this profile access the entered user ID in the local system.
As an FTAC user you can only specify your own user ID here.
If the FTAC administrator has created an admission profile for a user without specifying the access data (see the CREATE-FT-PROFILE command in the openFT System Asministrator Guide), the user must, if necessary, enter the account and password in the operands ACCOUNT and PASSWORD described below before the profile can be used.

USER-ADMISSION = *UNCHANGED
The USER-ADMISSION of this admission profile remains unchanged.

USER-ADMISSION = *OWN
For USER-IDENTIFICATION and ACCOUNT, the specifications are taken from the current LOGON authorization. A BS2000 password is only taken from your LOGON authorization when an FT request accesses the admission profile.

USER-ADMISSION = *PARAMETERS(...)
Specifies the individual components of the user ID.

USER-IDENTIFICATION =
Your user ID in BS2000.

USER-IDENTIFICATION = *OWN
The user ID is taken from your LOGON authorization.

USER-IDENTIFICATION = <name 1..8>
User ID with which the profile is to be associated. As FTAC administrator you may also specify foreign user IDs.

ACCOUNT =
Account number under which an FT request is to be kept when it uses this admission profile.

ACCOUNT = *OWN
The account number is taken from the current LOGON authorization.

ACCOUNT = *FIRST
The first account number assigned to the home pubset of the specified USER-IDENTIFICATION at the time the profile is used in the system is used for account assignment in the case of transfer requests. If the ID's account number changes, the profile has not to be modified.

ACCOUNT = *NOT-SPECIFIED
No account number is defined.
The account number is to be specified by the owner of the admission profile. This function permits the FTAC administrator to set up profiles for user IDs whose account numbers he/she does not know.

ACCOUNT = *NONE
The account number is used which is defined as the default account number of the user ID specified at the time the admission profile is used.

ACCOUNT = <alphanum-name 1..8>
An FT request should be kept under the account number specified when it accesses this admission profile. You can enter any account number which is associated with your user ID.

PASSWORD =
Password which an FT request is to use when it works with this admission profile.

PASSWORD = *OWN
When an FT request refers to this admission profile, FTAC uses the password valid for the specified USER-IDENTIFICATION at that moment. This prevents you from having to modify the admission profile if the BS2000 password is changed.

PASSWORD = *NOT-SPECIFIED
The password is specified by the owner of the admission profile. This function permits the FTAC administrator to set up profiles for foreign user IDs whose access data he/she does not know.

PASSWORD = <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
When an FT request accesses the admission profile, the specified password is compared with the current LOGON password. If the two do not correspond, the FT request is rejected.

PASSWORD = *NONE
No password is required for the user ID.

PASSWORD = *SECRET
The system prompts you to enter the password. However, this does not appear on the screen.

INITIATOR =
Determines if initiators from local and/or remote systems are permitted to use this admission profile for their FT requests.

INITIATOR = *UNCHANGED
The settings in this admission profile remain unchanged,

INITIATOR = *REMOTE
This admission profile may only be used for FT requests by initiators from remote systems.

INITIATOR = *LOCAL
This admission profile may only be used for FT requests by initiators from the local system.

INITIATOR = (*LOCAL,*REMOTE)
This admission profile may be used by initiators from local and remote systems.

TRANSFER-DIRECTION =
Determines which transfer direction may be used with this admission profile.

ℹ The transfer direction is always determined from the system in which the admission profile was defined.

TRANSFER-DIRECTION = *UNCHANGED
The specification in the admission profile remains unchanged.

TRANSFER-DIRECTION = *NOT-RESTRICTED
Files can be transferred to and from a partner system.

TRANSFER-DIRECTION = *FROM-PARTNER
Files can only be transferred from a partner system to your system. It is not possible to display file attributes/directories (partial components of “inbound file management”).

TRANSFER-DIRECTION = *TO-PARTNER
Files can only be transferred from your system to a partner system. It is not possible to modify file attributes or delete files (partial components of “inbound file management”).

PARTNER =
Specifies that this admission profile is to be used only for FT requests which are processed by a a certain partner system.

PARTNER = *UNCHANGED
Any partner in the admission profile remains unchanged.

PARTNER = *NOT-RESTRICTED
This admission profile’s scope of use is not limited to FT requests with certain partner systems.

PARTNER = *ADD(NAME = list-poss(50): <text 1..200 with-low>)
With this specification, you can add elements to an existing list of partner systems.
A maximum of 50 partner systems can be specified.

PARTNER = *REMOVE(NAME = list-poss(50): <text 1..200 with-low>)
Removes elements from an existing list of partner systems. A maximum of 50 partner systems can be specified.

PARTNER = list-poss(50): <text 1..200 with-low>
The admission profile only permits those FT requests which are processed with the specified partner systems. A maximum of 50 partner systems can be specified.
For PARTNER you can specify the name from the partner list or the address of the partner system, see also section “Specifying partner addresses” on page 44. You are advised to use the name from the partner list.

MAX-PARTNER-LEVEL =
A maximum security level can be specified. The admission profile will then only permit those FT requests which are processed with partner systems which have this security level or lower.
MAX-PARTNER-LEVEL works in conjunction with the admission set. When non-privileged admission profiles are used, the access check is executed on the basis of the smallest specified value.

MAX-PARTNER-LEVEL = *UNCHANGED
The specification for MAX-PARTNER-LEVEL in this admission set remains unchanged.

MAX-PARTNER-LEVEL = *NOT-RESTRICTED
If FT requests are processed with this admission profile, then the highest accessible security level is determined by the admission set.

MAX-PARTNER-LEVEL = <integer 0..100>
All partner systems which have this security level or lower can be communicated with.

i When you set MAX-PARTNER-LEVEL=0, you prevent access to the admission profile (for the time being). No FT request can then be processed with this admission profile.

FILE-NAME =
Determines which files or library members under your user ID may be accessed by FT requests that use this admission profile.

FILE-NAME = *UNCHANGED
The specifications for FILE-NAME in this admission profile remain unchanged.

FILE-NAME = *NOT-RESTRICTED
The admission profile permits unrestricted access to all files and library members of the user ID.

**FILE-NAME = <filename 1..54> / <c-string 1..512 with-low> /
*POSIX(NAME = <posix-pathname 1..510>)**
Only the specified file may be accessed. However, openFT is also able to generate unique filenames automatically, thus providing an easy way of avoiding conflicts. This is done by specifying the string %UNIQUE at the end of the filename which is predefined here (see the section “File names” in the User Guide). When follow-up processing is specified, this file can be referenced with %FILENAME.
You can also directly specify file transfer with pre- and post-processing here by entering the pipe symbol ’|’ followed by a command.

**FILE-NAME =*EXPANSION(PREFIX = <filename 1..53> /
<partial-filename 2..53> / <c-string 1..511 with-low>)**
Restricts access to a number of files which all begin with the same prefix. If a *filename* is entered in an FT request which uses this admission profile, FTAC sets the *prefix* defined with EXPANSION in front of this filename. The FT request is then permitted to access the file *PrefixFilename*.

Example

– PREFIX=STEVEN.; An FT request in which the FILE-NAME=MILLER is specified accesses the file STEVEN.MILLER.

Please note that the part of a DVS filename which is specified in the file transfer command still has to be of the type <filename>.

If you want to perform file transfer with pre- or post-processing, you should indicate this by entering the pipe symbol ‘|’ at the start of the prefix. The created FTAC profile can then be used only for file transfer with pre- or post-processing since the file name that is generated also starts with a ‘|’. The variable %TEMPFILE can also be used in the filename prefix. You can find detailed information on preprocessing and postprocessing in the section of the same name in the User Guide.

The maximum length of the entire pre- or post-processing command is limited to the maximum length of the file name. If several commands are specified, then they must be separated by a semicolon (‘;’).
There must not be a space between the semicolon and the slash.

Example

```
FILE-NAME = C‘|/Command1;/Command2;/Command3; ...‘
```

If you specify a name prefix that starts with a pipe character with *EXP(PREFIX=...), the preprocessing or postprocessing command of the FT request must not contain any semicolons. If the preprocessing or postprocessing command nevertheless contains semicolons, it must be enclosed in '...' (single quotes) or "..." (double quotes).

Special cases

– In the case of admission profiles which are to be used exclusively for the ftexec command you must specify a filename or filename prefix that starts with the character string ‘|ftexecsv’ (see CREATE-FT-PROFILE , “Example 3” on page 177).

– Specify the file name prefix '|*ftmonitor' for admission profiles that are exclusively used for monitoring. A profile of this sort can then be used in the openFT Monitor or in an ft or ncopy command from a Windows or Unix system (see page 79 and “Example 2” on page 177).

FILE-NAME = *LIBRARY-ELEMENT(...)
Determines which of your libraries and library members may be accessed by FT requests which use this admission profile.

LIBRARY =
Defines which libraries may be accessed with this admission profile.

LIBRARY = *UNCHANGED
The library specifications in the admission profile remain unchanged.

LIBRARY = *NOT-RESTRICTED
The admission profile does not restrict access to libraries.

LIBRARY = <filename 1..54>
Only this library may be accessed.

LIBRARY = *EXPANSION(PREFIX = <composed-name 1..63 with-under> / <partial-filename 2..63>)
Only those libraries may be accessed which begin with the specified prefix. FTAC sets the prefix in front of a library name in an FT request which uses this admission profile, and then permits access to the library *Prefix-Libraryname*.

ELEMENT =
Determines which library members may be accessed with this admission profile.

ELEMENT = *UNCHANGED
The library member specifications in the admission profile remain unchanged.

ELEMENT = *NOT-RESTRICTED
Permits unrestricted access to library members.

ELEMENT = <composed-name 1..64 with-under>(...)
Only permits access to the specified library member.

VERSION =
Access is only permitted for a specific version of the library member.

VERSION = *STD
Permits access only to the highest version of the library member.

VERSION = <text 1..24>
Access is only permitted for this version of the library member.

ELEMENT = *EXPANSION(PREFIX = <composed-name 1..63 with-under> / <partial-filename 2..63>)
Defines a prefix. When a name for a library member is specified in an FT request which uses this admission profile, FTAC adds the specified prefix to this member name. The admission profile then permits access to this member with the name *PrefixElementname*.

TYPE =
Specifies a certain type of library member. The admission profile then only permits access to library members of this type.

TYPE = *UNCHANGED
Any access restrictions to individual member types remain unchanged.

TYPE = *NOT-RESTRICTED
Access is not restricted to a certain type of library member.

TYPE = <name 1..8>
FT requests which use this admission profile may only access library members of this type.

FILE-PASSWORD =
You can enter a password for files into the admission profile. The FTAC functionality then only permits access to files which are protected with this password and to unprotected files. When a FILE-PASSWORD is specified in an admission profile, the password may no longer be specified in an FT request which uses this admission profile. This allows you to permit access to certain files to users in remote systems, without having to disclose the file passwords.

FILE-PASSWORD = *UNCHANGED
The specifications for FILE-PASSWORD in this admission profile remain unchanged.

FILE-PASSWORD = *NOT-RESTRICTED
Permits access to all files. If a password is set for a file, then it must be specified in the transfer request.

FILE-PASSWORD = *NONE
Only permits access to files without file passwords.

FILE-PASSWORD = <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
Only permits access to files which are protected with the password specified and to unprotected files. The password which has already been specified in the profile may not be repeated in the transfer request. PASSWORD=*NONE would be entered in this case!

FILE-PASSWORD = *SECRET
The system prompts you to enter the password. However, this does not appear on the screen.

PROCESSING-ADMISSION =
You can enter a user ID in your BS2000 system. Any follow-up processing of an FT request will be executed under this user ID. With PROCESSING-ADMISSION in the admission profile, you do not need to disclose your LOGON authorization to partner systems for follow-up processing.

PROCESSING-ADMISSION = *UNCHANGED
The PROCESSING-ADMISSION in this admission profile remains unchanged.

PROCESSING-ADMISSION = *SAME
For the PROCESSING-ADMISSION, the values of the USER-ADMISSION are used. If *SAME is entered here, then any FT request which uses this profile must also contain PROCESSING-ADMISSION=*SAME or PROCESSING-ADMISSION= *NOT-SPECIFIED. The entry *SAME is only possible here if the follow-up processing is not started with the command /ENTER.

PROCESSING-ADMISSION = *NOT-RESTRICTED
FT requests which use this admission profile may contain any PROCESSING-ADMISSION. For follow-up processing with FTAM partners, PROCESSING-ADMISSSION must have a value not equal to *NOT-RESTRICTED.

PROCESSING-ADMISSION = *PARAMETERS(...)
You can also enter the individual components of the user ID. This allows follow-up processing using this admission profile and started from FT requests to be charged under a different account number, for example. Or, a password can be set in the admission profile. Follow-up processing for FT requests which use this admission profile will then only function if their current LOGON password corresponds to the pre-set password.

USER-IDENTIFICATION =
User ID under which the follow-up processing is to be executed.

USER-IDENTIFICATION = *SAME
The USER-IDENTIFICATION is taken from the USER-ADMISSION.

USER-IDENTIFICATION = *NOT-RESTRICTED
The admission profile does not restrict the user ID under which the follow-up processing is to be executed.

USER-IDENTIFICATION = <name 1..8>
FT requests which are processed with this admission profile are only permitted follow-up processing under this user ID. If another user ID is entered here, the parameter PASSWORD must also be entered. PASSWORD=*SAME is then not valid.

ACCOUNT =
Specifies the account number for the follow-up processing.

ACCOUNT = *SAME
The account number is taken from the USER-ADMISSION.

ACCOUNT = *NOT-RESTRICTED
The account number may be specified in FT requests that work with the admission profile. The admission profile does not restrict the account for follow-up processing.

ACCOUNT = *NONE
The account number is used which is defined as the default account number of the user ID specified at the time the admission profile is used.

ACCOUNT = <alphanum-name 1..8>
Follow-up processing is to be settled under this account number.

PASSWORD =
Specifies, where applicable, the BS2000 password for the user ID under which the follow-up processing is to be executed. Here, you can enter a PASSWORD when the user ID in question doesn’t have such a password (yet).

PASSWORD = *SAME
The value *SAME is only valid if the PROCESSING-ADMISSION refers to your own user ID. If PASSWORD=*OWN is entered on USER-ADMISSION, then the BS2000 password valid at the time of the request is used for the PROCESSING-ADMISSION. The entry *SAME is only possible here if the follow-up processing is not started with the command /ENTER.

PASSWORD = *NOT-RESTRICTED
The password may be specified for FT requests which work with the admission profile. The admission profile does not restrict the password for follow-up processing.

PASSWORD = *NONE
FT requests which use this admission profile can only initiate follow-up processing on user IDs without a password.

PASSWORD = <c-string 1..8> / <c-string 9..32> / <x-string 1..16>
FT requests which use the admission profile may only initiate follow-up processing on user IDs which are protected with this password.

PASSWORD = *SECRET
The system prompts you to enter the password. The entry does not appear on the screen.

SUCCESS-PROCESSING =
Restricts the follow-up processing which an FT request is permitted to initiate in your system after a successful data transfer.

SUCCESS-PROCESSING = *UNCHANGED
The specifications for SUCCESS-PROCESSING in this admission profile remain unchanged.

SUCCESS-PROCESSING = *NOT-RESTRICTED
In FT requests which use this admission profile the operand SUCCESS-PROCESSING may be used without restriction.

SUCCESS-PROCESSING = *NONE
The admission profile does not permit follow-up processing after successful data transfer.

SUCCESS-PROCESSING = <c-string 1..1000 with-low>
BS2000 commands which are executed in the local system after successful data transfer. Individual commands must be preceded by a slash (/).
The individual commands must be separated by a semicolon (;). If a character string is enclosed by single or double quotes (’ or ”) within a command sequence, openFT does not interpret any semicolons within this character string as a separator.

SUCCESS-PROCESSING = *EXPANSION(...)
If a SUCCESS-PROCESSING was specified in an FT request which uses this admission profile, FTAC adds the prefix or suffix specified here to this command. As follow-up processing, the command which has been thus expanded is then executed.

If a suffix or prefix is defined at this point, then no command sequence for the follow-up processing may be specified in FT requests which use this admission profile. This makes the setting of prefixes and suffixes mandatory.

PREFIX = *UNCHANGED
The specifications for the follow-up processing prefix in this admission profile remain unchanged.

PREFIX = *NOT-RESTRICTED
Follow-up processing is not restricted by a prefix.

PREFIX = <c-string 1..999 with-low>
The specified prefix is set in front of a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the prefix is executed as follow-up processing.

SUFFIX = *UNCHANGED
The specifications for the follow-up processing suffix in this admission profile remain unchanged.

SUFFIX = *NOT-RESTRICTED
Follow-up processing is not restricted by a suffix.

SUFFIX = <c-string 1..999 with-low>
The specified prefix is set after a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the suffix is executed as follow-up processing.

Example

- If PREFIX='/PRINT-FILE ' is defined and SUCC='filename' specified in the FT request, then FT executes the command “/PRINT-FILE filename” as follow-up processing.
- If SUFFIX='filename' is defined and SUCC='/PRINT-FILE' specified in the FT request, then FT executes the command “/PRINT-FILE filename” as follow-up processing.

FAILURE-PROCESSING =
Restricts the follow-up processing which an FT request is permitted to initiate in your system after a failed data transfer.

FAILURE-PROCESSING = *UNCHANGED
The specifications for FAILURE-PROCESSING in this admission profile remain unchanged.

FAILURE-PROCESSING = *NOT-RESTRICTED
In FT requests which use this admission profile the operand FAILURE-PROCESSING may be used without restriction.

FAILURE-PROCESSING = *NONE
The admission profile does not permit follow-up processing after failed data transfer.

FAILURE-PROCESSING = <c-string 1..1000 with-low>
BS2000 commands which are executed in the local system after failed data transfer. Individual commands must be preceded by a slash (/). The individual commands must be separated by a semicolon (;). If a character string is enclosed by single or double quotes (’ or ”) within a command sequence, openFT does not interpret any semicolons within this character string as a separator.

FAILURE-PROCESSING = *EXPANSION(...)
If a FAILURE-PROCESSING was specified in an FT request which uses this admission profile, FTAC adds the prefix or suffix specified here to this command. As follow-up processing, the command which has been thus expanded is then executed.

If a suffix or prefix is defined at this point, then no command sequence for the follow-up processing may be specified in FT requests which use this admission profile. This makes the setting of prefixes and suffixes mandatory.

PREFIX = *UNCHANGED
The specifications for the follow-up processing prefix in this admission profile remain unchanged.

PREFIX = *NOT-RESTRICTED
Follow-up processing is not restricted by a prefix.

PREFIX = <c-string 1..999 with-low>
The specified prefix is set in front of a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the prefix is executed as follow-up processing.

SUFFIX = *UNCHANGED
The specifications for the follow-up processing suffix in this admission profile remain unchanged.

SUFFIX = *NOT-RESTRICTED
Follow-up processing is not restricted by a suffix.

SUFFIX = <c-string 1..999 with-low>
The specified prefix is set after a command which is specified in an FT request as follow-up processing. Then, the command which has been expanded with the suffix is executed as follow-up processing.

WRITE-MODE =
Determines the WRITE-MODE which is valid for this FT request. WRITE MODE is only effective if the receive file is in the same system as the admission profile definition.

WRITE-MODE = *UNCHANGED
The specifications for WRITE-MODE in this admission profile remain unchanged.

WRITE-MODE = *NOT-RESTRICTED
In an FT request which accesses this admission profile, WRITE-MODE may be used without restrictions.

WRITE-MODE = *NEW-FILE
In the FT request, *NEW-FILE, *REPLACE-FILE or *EXTEND-FILE may be entered for WRITE-MODE. If the receive file already exists, the transfer will be rejected.

WRITE-MODE = *REPLACE-FILE
In the FT request of openFT or FTAM partners, only *REPLACE-FILE or *EXTEND-FILE may be entered for WRITE-MODE. With ftp partners, *NEW-FILE may also be entered if the file does not yet exist.

WRITE-MODE = *EXTEND-FILE
In the FT request, only *EXTEND-FILE may be entered for WRITE-MODE.

FT-FUNCTION =
This operand permits the restriction of the profile validity to certain FT functions (=file transfer and file management functions).

FT-FUNCTION = *UNCHANGED
The previous scope of the FT functions remains unchanged.

FT-FUNCTION = *NOT-RESTRICTED
The full scope of FT functions is available with the exception of the “remote administration” function (*REMOTE-ADMINISTRATION). This must be activated explicitly.

FT-FUNCTION = (*TRANSFER-FILE, *MODIFY-FILE-ATTRIBUTES, *READ-DIRECTORY, *FILE-PROCESSING, *REMOTE-ADMINISTRATION)
The following file transfer functions are available:

***TRANSFER-FILE**
The admission profile may be used for the file transfer functions “transfer files”, “view file attributes” and “delete files”.

***MODIFY-FILE-ATTRIBUTES**
The admission profile may be used for the file transfer functions “view file attributes” and “modify file attributes”.

***READ-DIRECTORY**
The admission profile may be used for the file transfer functions “view directories” and “view file attributes”.

***FILE-PROCESSING**
The admission profile may be used for the “pre-processing” and “post-processing” file transfer functions. The “transfer files” function must also be permitted.

The *FILE-PROCESSING specification is of relevance only for FTAC profiles without a filename prefix. Otherwise the first character of the filename prefix determines whether only normal data transfer (no pipe symbol “|”) or only pre- and post-processing (pipe symbol “|”) are to be possible with this FTAC profile.

***REMOTE-ADMINISTRATION**
The admission profile is allowed to be used for the "remote administration" function. This allows a remote administrator to administer the openFT instance using this profile. *REMOTE-ADMINISTRATION may only be specified by the FT administrator or FTAC administrator.

USER-INFORMATION =
Specifies a text in the admission profile. This text can be displayed with the SHOW-FT-PROFILE command.

USER-INFORMATION = *UNCHANGED
Any existing text remains unchanged.

USER-INFORMATION = *NONE
Any existing text is deleted.

USER-INFORMATION = <c-string 1..100 with-low>
The character string entered is accepted as user information.

DATA-ENCRYPTION =
Specifies whether user data with this profile must be transferred in encrypted form.

DATA-ENCRYPTION = *UNCHANGED
The encryption option should remain unchanged.

DATA-ENCRYPTION = *NOT-RESTRICTED
The encryption option for user data is not restricted. File transfer requests with encryption and file transfer requests without encryption are both accepted

DATA-ENCRYPTION = *NO
Only file transfer requests that do not have encrypted user data are accepted, i.e. requests with encryption are rejected. If the request is made in a BS2000 or z/OS, DATA-ENCRYPTION=*NO must be specified there in the NCOPY request.

DATA-ENCRYPTION = *YES
Only file transfer requests that have encrypted user data are accepted, i.e. requests without encryption are rejected. If the request is made in a BS2000 or z/OS, for example, then DATA-ENCRYPTION=*YES must be specified there in the NCOPY request.

i When using restrictions for FILE-NAME, SUCCESS-PROCESSING and FAILURE-PROCESSING, keep in mind that

- a restriction for follow-up processing must always be made for SUCCESS- and FAILURE-PROCESSING. Otherwise, it is possible that users will avoid this step.
- PREFIX of FILE-NAME, SUCCESS-PROCESSING and FAILURE-PROCESSING must correspond,
  e.g. FILE-NAME = *EXP(XYZ.),SUCC = *EXP('/PRINT-FILE XYZ.')

Example

After Steven Miller has created an admission profile with the name *profile1*, which permits other users access to his user ID with the LOGON authorization, he decides he wants to restrict this profile so that only FT accesses are possible to files which begin with the prefix *BRANCH*.

The required command is:

```
/MODIFY-FT-PROFILE␣NAME = profil1,
          FILE-NAME = *EXPANSION(PREFIX = branch.)
```

A possible short form of this command is:

```
/MOD-FT-PROF␣profil1,FILE-N = (PRE = branch.)
```

This places heavy restrictions on the admission profile. The other specifications remain unchanged.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	FTC0051	A user ID with the same name already exists.
0	64	FTC0053	No FT profile exists which meets the criteria specified.
0	64	FTC0055	The partner restrictions were lifted.
0	0	FTC0056	Transfer admission is blocked.
0	64	FTC0100	An FT profile with this name already exists.
0	64	FTC0101	An FT profile with the specified transfer admission already exists.
0	64	FTC0150	The access password is missing.
0	64	FTC0151	Modifications can only be made by the administrator or owner.
0	64	FTC0153	The owner ID entered is not the user’s own ID.
0	64	FTC0170	The partner entered is unknown within the partner system available for this user.
0	64	FTC0171	The profile entered does not exist.
0	64	FTC0172	The user admission entered does not exist in the system.
0	64	FTC0173	The processing admission entered does not exist in the system.
0	64	FTC0174	The parameters “NEW-NAME” and “TRANSFER-ADMISSION” may only used together in conjunction with unique selection criteria (“NAME” or “TRANSFER-ADMISSION”).
0	64	FTC0178	The partner name entered occurs several times.
0	64	FTC0179	The maximum number of partner restrictions has been exceeded.
0	64	FTC0182	The maximum length of partner names has been exceeded.
0	64	FTC0200	The total length of the two follow-up processing commands is too long.
0	64	FTC0255	A system error has occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.27 REMOVE-FT-PARTNER Remove remote system from partner list

Note on usage

User group: FT administrator

Alias name: FTREMPTN

Functional description

The REMOVE-FT-PARTNER command is used to remove a remote system from the partner list of the local system.

If a partner system is deleted from the partner list then all requests involving this partner system are aborted. REMOVE-FT-PARTNER therefore represents a simple way to delete all the requests relating to a given partner. A request to a partner removed with REMOVE-FT-PARTNER is eliminated even if the request is already known in the partner system (in the same way as with CANCEL-FILE-TRANSFER .. FORCE-CANCELLATION=*YES).

Format

REMOVE-**FT-PART**NER / **FTREMPTN**
PARTNER = <text 1..200 with-low>

Operands

PARTNER = <text 1..200 with-low>
Name of the partner system from the partner list or the address of the partner system.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
35	64	FTR1035	Command only permissible for FT administrator.
45	64	FTR1045	Partner name not found in partner list.
1	0	FTR1048	Active requests could not yet be deleted.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

Remove the remote system PARTNER1 from the partner list of the local system:

```
/REMOVE-FT-PARTNER PARTNER=PARTNER1
```

5.28 SHOW-FILE-TRANSFER Query status of file transfer request

Note on usage

User group: FT user and FT administrator

Alias names: SHFT / NSTATUS / FTSHWREQ

Functional description

The SHOW-FILE-TRANSFER command allows you to request information about FT requests. As with CANCEL-FILE-TRANSFER , you can specify selection criteria in order to obtain information about specific FT requests.

The FT administrator can obtain information about the requests of any owner.

The owner of requests issued in the local system is the user ID under which they are submitted. The owner of requests issued in the remote system is the user ID in the local system under which the requests are executed.

The scope of information to be output can be selected. By default the following information is output by the system in response to the SHOW-FILE-TRANSFER command:

- the transfer ID of the request,
- the initiator of the request (local or remote system),
- the operating status of the request (see description of operands for more details),
- the partner system,
- the transfer direction,
- the name of the file (or library member) to be transferred in the local system.
- the number of bytes transferred

By entering INFORMATION=*ALL in the SHOW-FILE-TRANSFER command more information can be obtained. openFT then, in addition to the standard output, outputs the values of further operands of the transfer command that was used to issue the request. Which output parameters are displayed depends on the parameters which were specified for the request.

The complete description of all possible output parameters and values is provided in the section “Meaning of the fields in the long output” on page 298.

The more precise your information request, the fewer irrelevant requests are output.

When you specification of INFORMATION=*SUMMARY returns a small table with the number of jobs in the various request states.

Format

```
SHOW-FILE-TRANSFER / SHFT / NSTATUS / FTSHWREQ

 TRANSFER-ID = *ALL / <integer 1..2147483647>
,SELECT = *OWN / *PARAMETERS(...)
   *PARAMETERS(...)
     | OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
     |,INITIATOR = (*LOCAL, *REMOTE) / list-poss(2): *LOCAL / *REMOTE
     |,PARTNER = *ALL(...) / <text 1..200 with-low>
     |    *ALL(...)
     |      | PARTNER-STATE = *ALL / *ACTIVE
     |,FILE-NAME = *ALL / <filename 1..54> / <c-string 1..512 with-low> /
     |                  *LIBRARY-ELEMENT(...) / *POSIX(NAME=<posix-pathname 1..510>) /
     |                  *PUBSET(PUBSET=<cat-id 1..4>)
     |    *LIBRARY-ELEMENT(...)
     |      | LIBRARY = *ALL / <filename 1..54>
     |      |,ELEMENT = *ALL / <filename 1..64 without-gen-vers>(...) /
     |      |                  <composed-name 1..64 with-under>(...)
     |      |    <filename>(...) / composed-name>(...)
     |      |      | VERSION = *ALL / <text 1..24>
     |      |,TYPE = *ALL / <name 1..8>
     |,MONJV = *NONE / <filename 1..54 without-gen-vers>
     |,JV-PASSWORD = *NONE / <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647> /
     |                  *SECRET
     |,STATE = *ALL / *SUSPEND / *LOCKED / *WAIT / *ACTIVE / *CANCELLED / *FINISHED / *HOLD
     |,GLOBAL-REQUEST-ID = *ALL / <alphanum-name 1..10>
,INFORMATION = *STD / *ALL / *SUMMARY
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
   *SYSOUT(...) / *SYSLST(...)
     | LAYOUT = *STD / *CSV
```

Operands

TRANSFER-ID =
Transfer ID of the FT request about which information is required.

TRANSFER-ID = <u>*ALL</u>
Supplies information about all the owner’s FT requests.
The FT administrator can obtain information about all current FT requests that access his/her system.

TRANSFER-ID = <integer 1..2147483647>
Transfer ID assigned to the local system and output as part of the message confirming acceptance of the request.

SELECT =
Contains selection criteria defining the file transfer requests on which inquiries are to be made. Information on a file transfer request is output if the request satisfies all the specified criteria.

SELECT = *OWN
Provides information on all current file transfer requests for which you are designated as the owner.

SELECT = *PARAMETERS(...)

OWNER-IDENTIFICATION =
Owner of the FT requests. Only the FT administrator can make use of this operand unrestricted.

OWNER-IDENTIFICATION = *OWN
Provides information only on the file transfer requests in the user's own ID.

OWNER-IDENTIFICATION = *ALL
Provides information on FT requests in all user IDs.

OWNER-IDENTIFICATION = <name 1..8>
Specific user ID about whose file transfer requests information is required.

INITIATOR =
Initiator of the file transfer requests concerned.

INITIATOR = (*LOCAL,*REMOTE)
Provides information on file transfer requests in the local system and in remote systems.

INITIATOR = *LOCAL
Provides information on file transfer requests issued in the local system.

INITIATOR = *REMOTE
Provides information on file transfer requests issued in the remote systems.

PARTNER =
Selects file transfer requests carried out with a specified remote system.

PARTNER = *ALL(...)
The partner system is not used as a selection criterion to determine the file transfer requests on which information is to be output.

PARTNER-STATE =
The status of the partner system is used as a selection criterion.

PARTNER-STATE = *ALL
The requests are selected independently of the partner system's status.

PARTNER-STATE = *ACTIVE
Only the requests to and from the active partners are selected.

PARTNER = <text 1..200 with-low>
Name or an address of a partner system. Information is required on the file transfer requests being executed with this system. For more information on address specifications, see section "Defining partner properties" on page 44.

FILE-NAME =
FT requests that access this file, this pubset or this library member in the local system as a send file or receive file. The file name or library member name must be specified exactly as it appears in the FT request. If %UNIQUE was specified, the file name generated by openFT must be entered as the selection criterion here.

FILE-NAME = *ALL
The file name is not used as a selection criterion to define the file transfer requests on which information is to be output.

FILE-NAME = <filename 1..54> / <c-string 1..512 with-low> /
***POSIX(NAME = <posix-pathname 1..510>)**
Name of a file. Information is required on the file transfer requests that access this file.

FILE-NAME = *PUBSET(PUBSET = <cat-id 1..4>)
Information on all FT requests that have locked files on the specified pubset should be displayed.

FILE-NAME = *LIBRARY-ELEMENT(...)
Information is required on file transfer requests that access library members in the local system.

LIBRARY =
Selects the library concerned.

LIBRARY = *ALL
The library name is not used as a selection criterion to define the file transfer requests on which information is to be output.

LIBRARY = <filename 1..54>
Name of a library. Information is required on the file transfer requests that access this library.

ELEMENT =
Library member. Information is required on all the file transfer requests that access this member.

ELEMENT = *ALL
The name of the library member is not used as a selection criterion to define the file transfer requests.

ELEMENT = <filename 1..64 without-gen-vers>(...) / <composed-name 1..64 with-under>(...)
Name of a library member. Information is required on the file transfer requests that access this library member.

VERSION =
Version number of the library member.

VERSION = *ALL
Information is required on all file transfer requests that access any version of the library member.

VERSION = <text 1..24>
Information is required on the file transfer requests that access a specific version of the library member.

TYPE =
The type of library member.

TYPE = *ALL
The member type is not used as a selection criterion to define the file transfer requests on which information is to be output.

TYPE = <name 1..8>
Information is required only on those file transfer requests that access library members of this type.

MONJV =
If appropriate, selects the specific file transfer request that is being monitored by this job variable.

MONJV = *NONE
A job variable is not used as a selection criterion to define the file transfer request on which information is to be output.

MONJV = <filename 1..54 without-gen-vers>
Information is required on the file transfer request that is being monitored by this job variable.

JV-PASSWORD =
If required, specifies the password needed to access the job variable.

If you have already notified the system of the password with the BS2000 command ADD-PASSWORD, you do not have to specify JV-PASSWORD.

JV-PASSWORD = *NONE
The job variable is not password-protected.

JV-PASSWORD = <c-string 1..4> / <x-string 1..8> / <integer -2147483648..2147483647>
This password is required for the job variable.

JV-PASSWORD = *SECRET
The system requests you to enter the password. This input is not displayed on the screen.

STATE =
Selects those file transfer requests that are in the specified status. The status of a request may change in between entry of the command and information output. This is why the output may include requests that are in a state other than the one selected with STATE.

STATE = *ALL
The status of a request is not used as a selection criterion to define the file transfer requests on which information is to be output.

STATE = *SUSPEND
Requests information on those file transfer requests that are currently in SUSPEND status (= interrupted).

STATE = *LOCKED
Requests information on FT requests that are in the LOCKED operating status (= temporarily locked as a result of a longer term resource bottleneck).

STATE = *WAIT
Requests information on those file transfer requests that are currently in WAIT status (= waiting for resources).

STATE = *ACTIVE
Requests information on those file transfer requests that are currently in ACTIVE status (= being processed).

STATE = *CANCELLED
Requests information on those file transfer requests that were canceled and are waiting for negotiation with the communications partner to be concluded. These requests are visible only to the FT administrator.

STATE = *FINISHED
Requests information on those file transfer requests that are currently in FINISHED status (= terminated or aborted, but where the user has not yet been informed).

STATE = *HOLD
Requests information on those FT requests that are currently in HOLD status (= awaiting the specified start time).

GLOBAL-REQUEST-ID =
Selects the FT requests on the basis of the global request identification.

GLOBAL-REQUEST-ID = *ALL
The global request identification is not a search criterion.

GLOBAL-REQUEST-ID = <alphanum-name 1..10>
Requests information on the FT request with a particular global request identification. The global request identification is relevant only for inbound requests of openFT and FTAM partners. It is assigned by the initiator of the request (transfer ID) and transferred to the local system.

INFORMATION =
Scope of the output.

INFORMATION = *STD
Output is summary form and contains the following information (see “Description of the short output” on page 295):

- Transfer ID,
- Initiator,
- State of the request,
- Partner,
- Direction of transfer,
- Byte count,
- File or library member name in the local system.

INFORMATION = *ALL
Output is in full form. In addition to the summary form data, further information is provided on the operands used in the TRANSFER-FILE command (see “Description of the long output” on page 297).

INFORMATION = *SUMMARY
Output is in the form of a specified sum. By specifying INFORMATION=*SUMMARY, you can restrict the output information to a statistic of the currently existing requests. By doing this, the display is arranged according to the conditions in which the requests find themselves. The displayed sum can, of course, exceed the sum of the individual columns, since all requests, even those that still have no request condition, are counted. Information is output about the number of request in each individual processing status (see “Description of the summary output” on page 301).

OUTPUT =
Output medium.

OUTPUT = *SYSOUT(...)
Output is sent to SYSOUT.

OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = *STD
Output is formatted using a standard layout that can be easily read by the user.

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon “;“ (see section “Output in CSV format” on page 135).

If selection criteria are specified in the SHOW-FILE-TRANSFER command and no request is found that matches all the specified criteria, the command is acknowledged with the following message:

```
% FTR0504 No requests available for the selection criteria
```

In such a case, procedures do not branch to the next SET-JOB-STEP.

Commando return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	There are no requests that meet the specified selection criteria.
33	32	CMD0221	Request rejected. Internal error.
36	32	CMD0221	Request rejected. Request data inconsistent.
82	32	CMD0221	Internal error. Job variable not accessible.
83	32	CMD0221	Internal error.
88	32	CMD0221	Error during OPS generation.
36	64	FTR1036	User not authorized for other user IDs
47	64	FTR1047	The request with the specified transfer ID could not be found.
226	64	FTR2226	Job variable contents inconsistent.
227	64	FTR2227	Job variable not in use by openFT.
228	64	FTR2228	Job variable not found.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

The following table shows the OPS variables for the command SHOW-FILE-TRANSFER with the operand INF=*ALL. The underlined values are valid for the output with the operand INF=*STD. The table on page 295 shows the OPS variables for the output with the operand INF=*SUMMARY.

Element	Type	Output
TRANS-ID	Integer	
STA	String	*SUSPEND / *LOCK / *WAIT / *ACTIVE / *FINISH /* HOLD
BYTE-COUNT	Integer	
PRIO	String	*NORM / *HIGH / *LOW
INIT	String	*LOC / *REM
TRANS-DIRECT	String	*TO-PARTNER / *FROM-PARTNER
PARTNER-NAME	String	
COMPRESS	String	*NONE / *BYTE-REPETITION / *ZIP
DATA-ENC	String	*YES / *NO
DICHECK	String	*YES / *NO
WRITE-MODE	String	* REPL-FILE / *NEW-FILE / *EXT-FILE

Element	Type	Output
FILE-SIZE	String	Value
REC-SIZE	String	Value
REC-FORMAT	String	*STD / *VARIABLE / *FIXED /*UNDEFINED
START	Struct	
.DATE	String	*SOON / yyyy-mm-dd
.TIME	String	*SOON / hh:mm:ss
CANCEL	Struct	
.DATE	String	*NO / yyyy-mm-dd
.TIME	String	*NO / hh:mm:ss
OWNER	String	
DATA-TYPE	String	*CHAR / *BINARY / *NOT-SPEC
TRANSP	String	*YES / *NO
LOC-PAR	Struct	
.F-TYPE[1]	String	*FILE / *LIB
.F-NAME	String	
.LIB	String	
.ELEM	String	
.VERSION	String	
.TYPE	String	
.TRANS-ADMIS	Struct	
.USER-ID	String	
.ACCOUNT	String	
.PROF-NAME[2]	String	
.PROCESS-ADMIS	Struct	
.USER-ID	String	
.ACCOUNT	String	
.SUCC-PROCESS	String	*SECRET / success-processing
.FAIL-PROCESS	String	*SECRET / failure-processing
.LISTING	String	*NONE / *SYSLST / *LISTFILE / *FAIL-SYSLST / *FAIL-LISTFILE
.MONJV	String	
.CCS-NAME	String	*STD / value
REM-PAR	Struct	

Element	**Type**	**Output**
.F-TYPE [1]	String	*FILE / *LIB
.F-NAME	String	
.LIB	String	
.ELEM	String	
.VERSION	String	
.TYPE	String	
.TRANS-ADMIS	Struct	
.USER-ID [3]	String	*REM-PROF / user-id
.ACCOUNT [3]	String	*REM-PROF / account
.PROCESS-ADMIS	Struct	
.USER-ID	String	
.ACCOUNT	String	
.SUCC-PROCESS	String	*SECRET / success-processing
.FAIL-PROCESS	String	*SECRET / failure-processing
.CCS-NAME	String	*STD / value
TARGET	Struct	
.FILE-FORMAT	String	*SAME / *BLOCK / *SEQ
.REC-FORMAT	String	*SAME / *UNDEF
PROTECTION	String	*STD / *SAME
GLOBAL-REQ-ID	Integer	

[1] For F-Type=*FILE, LIB, ELEM, VERSION and TYPE are not displayed.

[2] USER-ID and ACCOUNT are not assigned if an FTAC profile is specified.

[3] Since this cannot be output when a remote FTAC transfer admission is specified, USER-ID and ACCOUNT are assigned with *REM-PROFILE in this case.

The following table shows the OPS variables for the output with the operand INF=*SUMMARY.

Element	Type	Output
NUM-ACTIVE	Integer	
NUM-WAIT	Integer	
NUM-LOCK	Integer	
NUM-SUSPEND	Integer	
NUM-HOLD	Integer	
NUM-FINISHED	Integer	
NUM-SUMM [1]	Integer	

[1] Grand total of all requests including the requests that are still not validated and therefore not counted in any of the other elements.

5.28.1 Description of the short output

Example 1

Information is to be output to SYSOUT on those FT requests submitted by the remote system ALFRED which require access to the file DRAISINE and are currently active. The required command is as follows:

```
/SHOW-FILE-TRANSFER                                                    -
/                  SELECT=(INITIATOR=*REMOTE,                          -
/                  PARTNER=ALFRED,                                     -
/                  FILE-NAME=DRAISINE,                                 -
/                  STATE=*ACTIVE)
```

The recommended short form of this command is as follows:

```
/SHFT SEL=(INIT=*REM,PART-NAME=ALFRED,FILE=DRAISINE,STATE=*ACT)
```

or

```
/NSTATUS SEL=(INIT=*REM,PART-NAME=ALFRED,FILE=DRAISINE,STATE=*ACT)
```

The FT administrator must specify the operand OWNER=*ALL by SELECT if he/she is not the owner of the file DRAISINE.

The information is then output in the following format, for example:

```
%TRANS-ID   INI STATE PARTNER  DIR  BYTE-COUNT  FILE-NAME
%528184     REM ACT   ALFRED   TO   14760       DRAISINE
```

The information is output to SYSOUT, since this is the default value for the output of inquiry information.

Description of the output columns:

`TRANS-ID:` Transfer ID of the file transfer request

`INI:` Initiator of the file transfer request : *REM* for REMOTE, *LOC* for LOCAL

`STATE:` State of the request (here *ACT* for ACTIVE, other outputs:

`SUSP` for SUSPEND,
Inbound request suspended, e.g. due to higher priority requests.

`LOCK` for LOCKED,

`WAIT` for WAIT,

`FIN` for FINISHED,

`HOLD` for HOLD

`PARTNER:` Symbolic name of the relevant partner system.

If the FT request is in the STATE=WAIT state, and there is no normal internal resource bottleneck, then the partner name is preceded by one of the following characters:

* The FT administrator of the local system has locked a resource.

! An attempt to set up a connection to the partner system failed (possibly because the remote system is not running, for example, or because FT has not been started there or, in the case of TCP/IP connections, because the port specification contains *BY-TRANSPORTSYSTEM and there is no BCMAP). This can also occur, if openFT has discovered an error during the internal check of transferred data integrity.

? Installation error.
Possible reasons:

- The PORT in BCMAP does not correspond to that in the partner entry. Check the installation.
- The authentication of the local or remote system has failed due to an unsuitable public key.

`DIR:` Transfer direction

`BYTE-COUNT:` Number of bytes transferred up to the last restart point (in the case of data compression this is the a number of bytes of compressed data)

`FILE-NAME:` Name of the relevant file or library member in the local system

5.28.2 Description of the long output

The long output is described using an example of an outbound request and an example of an inbound request.

Example 1 (Outbound request)

Full information is to be output to SYSLST via the FT request with transfer ID 721212. If the file transfer request was issued under the same user ID as that under which the inquiry is made, then the command is as follows:

```
/SHOW-FILE-TRANSFER                                                   -
/                  TRANSFER-ID=721212,                                -
/                  INFORMATION=*ALL,                                  -
/                  OUTPUT=*SYSLST
```

The recommended short form of this command is as follows:

```
/SHFT 721212,INF=*ALL,OUT=*SYSLST
```

The information output on SYSLST then has the following format, for example:

```
%TRANSFER-ID =721212      STORE  =12-07-11 14:09:35  FILESIZE=40960000
%   STATE    =WAIT        BYTECNT=2117632
%   INITIATOR=LOCAL       TRANS  =TO                 PRIO    =NORM
%   WRITE    =REPLACE     START  =SOON               CANCEL  =NO
%   COMPRESS =BYTE        DATA   =CHAR
%   TRANSP   =NO          ENCRYPT=YES                TABEXP  =NO
%   OWNER    =USER1       DICHECK=NO
%   PARTNER  =WIN01
%   PARTNER-STATE =ACT
%   PARTNER-PRIO  =NORM
%   LOC: FILE     =$USER1.FILE.GR
%        TRANS-ADM=(USER1,88888)
%        ASYN-MSG =ALL
%   REM: FILE     =TEST2
%        TRANS-ADM=REMOTE-PROFILE
```

Example 2 (Inbound request)

Full information is to be output to SYSLST on the FT request with transfer ID 983050. If the file transfer request was issued under the same user ID as that under which the inquiry is made, then the command is as follows:

```
/SHOW-FILE-TRANSFER                                                   -
/                  TRANSFER-ID=983050,                                -
/                  INFORMATION=*ALL,                                  -
/                  OUTPUT=*SYSLST
```

```
%TRANSFER-ID =983050      STORE  =12-07-11 14:09:36  FILESIZE=40960000
%   STATE    =WAIT        BYTECNT=1925120
%   INITIATOR=REMOTE      TRANS  =FROM               PRIO    =
%   WRITE    =REPLACE     START  =SOON               CANCEL  =NO
%   COMPRESS =BYTE        DATA   =CHAR               GLOB-ID =721212
%   TRANSP   =NO          ENCRYPT=YES                TABEXP  =NO
%   OWNER    =USER2       DICHECK=YES                RECFORM =VARIABLE
%   PARTNER  =WIN01
%   PARTNER-STATE =ACT
%   PARTNER-PRIO  =NORM
%   FILE     =TEST2
%   TRANS-ADM=LAST
```

Meaning of the fields in the long output

The list below describes all fields which can occur in the long output (according to lines). Which fields are output in each particular case depends on the type and the parameters of the request.

`TRANSFER-ID:` Transfer ID of the request

`STORE:` The time at which the request was entered in the request queue

`FILESIZE:` The size of the file in bytes. If the output is flagged with a "K" on the right, the output is in kilobytes. If the output is flagged with "M", the output is in megabytes. The size is only shown here if the request has already been active. In the case of receive requests, a value is only shown here if the partner also sends that value.

`STATE`: State of the request

`BYTECNT:` Number of bytes transferred up to the last restart form (in the case of data compression in compressed form)

`INITIATOR:` Initiator of the request

`TRANS:` Transfer direction, as seen from local system

`PRIO:` Priority with which the request is to be started;
here: `NORM` for NORMAL.

WRITE: Specifies if or when the receive file is to be overwritten or extended

START: Requested start time of the request
(SOON for “as soon as possible”)

CANCEL: Requested abortion time
(NO for “no abortion requested”)

COMPRESS: Specifies whether or not the file is to be transferred in compressed form

DATA: Type of file:

CHAR for text file

BIN for binary file

NOT-SPECIFIED
in TRANSFER-FILE (NCOPY), no DATA-TYPE was specified

USER for user format

GLOB-ID: Global request identification, displayed only in the case of inbound requests from openFT and FTAM partners (INITIATOR=REMOTE). This corresponds to the request identification (=TRANSFER-ID) on the initiator system.

TRANSP: Specifies whether the transfer is to be done in transparent format

ENCRYPT: Specifies whether the file content is to be transferred in encrypted form

TARGFORM: Format of the transferred file in the target system:

SEQ Sequential file format

BLOCK Block format

TRECFRM: Record format of the file in the target system:

STD The same record format as in the sending system

UNDEFINED
Undefined record format

OWNER: Owner of request in local system

DICHECK: Specifies whether data integrity is to be checked (YES) or not (NO)

PROTECT: Specifies whether the protection attributes of the file are transferred

PARTNER: Symbolic name of partner system participating in the request.
If the FT request is in the STATE=WAIT state, and there is no normal internal resource bottleneck, then the partner name is preceded by one of the following characters:

- * The FT administrator of the local system has locked a resource.

! An attempt to set up a connection to the partner system failed (possibly because the remote system is not running, for example, or because FT has not been started there or, in the case of TCP/IP connections, because the port specification contains *BY-TRANSPORTSYSTEM and there is no BCMAP). This can also occur, if openFT has discovered an error during the internal check of transferred data integrity.

? Installation error.
Possible reasons:

- The PORT in BCMAP does not correspond to that in the partner entry. Check the installation.
- The authentication of the local or remote system has failed due to an unsuitable public key

`PARTNER-STATE:`
Status of the partner. Possible values:

`ACT` Activated

`DEACT` Deactivated

`NOCON` No connection, for instance because the openFT server has not been started on the remote system.

`INSTERR`
There is an installation or configuration error (for example, the local system is not known to the partner or the address of the partner in the partner list is not valid) or authentication of one of the partners has failed or encryption is not available locally or on the partner system.

`PARTNER-PRIO:`
Prioritization of the partner when processing requests.
Possible values:

`LOW` The partner has low priority.

`NORM` The partner has normal priority.

`HIGH` The partner has high priority.

`LOC:` Specifications on the local system (LOCAL-PARAMETER).

The entry can include more than in this example; the keywords correspond to the recommended abbreviations of the keywords of the transfer command; the meaning of the operand is also to be found there.

`FILE:` Local file name

`ASYN-MSG:`
Specifies which request result leads to an asynchronous termination message. Possible values: ALL, FAIL.

`REM:` Specifications on the remote system (REMOTE-PARAMETER).

The entry can include more than in this example; the keywords correspond to the recommended abbreviations of the keywords of the transfer command; the meaning of the operand is also to be found there.

`FILE:` Remote file name

The following parameters are only output for locally issued requests.

`TRANS-ADM:`

Transfer admission (here for the remote system. Instead of the triplet user ID, account number and password where appropriate, REMOTE-PROFILE can also be output here if a remote FTAC FT profile is addressed. The equivalent also applies to entries in the local system.

`CCSN:` CCS name used in the local and/or remote system when reading the file.

5.28.3 Description of the summary output

You want to output information about the number of request in each individual processing status.

```
/SHFT INF=*SUMMARY
% ACT    WAIT    LOCK    SUSP   HOLD    FIN     TOTAL
%   3      5       0       0      0      0         10
```

There are three requests in the ACTIVE condition, and five in the WAIT condition. Two requests are still in protocol handling, therefore the sum is 10.

5.29 SHOW-FTAC-ENVIRONMENT Display saved admission profiles and sets

Note on usage

User group: FTAC administrator

openFT-AC must be installed to use this command.

Functional description

The FTAC administrator can use the command SHOW-FTAC-ENVIRONMENT to view admission profiles and sets which have been written in an export file using the command EXPORT-FTAC-ENVIRONMENT (see page 199). This function is particularly useful before the importing of the admission profiles and sets (see page 201).

Format

```
SHOW-FTAC-ENVIRONMENT

 FROM-FILE = <filename 1..54>
,USER-IDENTIFICATION = *ALL / list-poss(100): <name 1..8>
,SELECT-PARAMETER = *ALL / *PARAMETERS(...)
    *PARAMETERS(...)
     |  PROFILE-NAME = *ALL / *NONE / *STD / list-poss(100): <alphanum-name 1..8>
     | ,ADMISSION-SET = *YES / *NO
,INFORMATION = *ONLY-NAMES / *ALL
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
    *SYSOUT(...) / *SYSLST(...)
     |  LAYOUT = *STD / *CSV
```

Operands

FROM-FILE = <filename 1..54>
Name of the file (not a temporary file) from which the admission profiles and sets are to be displayed. If the file contains invalid data or access to the file is unsuccessful, the command is rejected with the message FTC0103.

USER-IDENTIFICATION =
User ID whose admission profiles and sets are to be displayed.

USER-IDENTIFICATION = *ALL
The admission profiles and sets of all users are to be displayed.

USER-IDENTIFICATION = list-poss(100): <name 1..8>
The admission profiles and sets of the user IDs specified (maximum 100) are to be displayed.

SELECT-PARAMETER =
Specifies whether only admission profiles, only admission sets or both are to be displayed. For the admission profiles, you can specify which ones are to be displayed.

SELECT-PARAMETER = *ALL
All admission profiles and sets associated with the user ID specified under USER-IDENTIFICATION are to be output on file.

SELECT-PARAMETER = *PARAMETERS(...)
Specifies which of the admission sets associated with the USER-IDENTIFICATION are to be specified.

PROFILE-NAME = *ALL
All admission profiles are displayed.

PROFILE-NAME = *NONE
No admission profiles are displayed.

PROFILE-NAME = *STD
Displays the default admission profile.

PROFILE-NAME = list-poss(100): <alphanum-name 1..8>
Only the specified profiles are displayed (maximum 100).

ADMISSION-SET = *YES
All admission sets are displayed.

ADMISSION-SET = *NO
No admission sets are displayed.

INFORMATION =
Scope of the information to be displayed.

INFORMATION = *ONLY-NAMES
Only the names of the admission profiles are to be displayed.

INFORMATION = *ALL
The entire contents of the admission profiles, excluding any passwords and transfer admissions, are displayed.

OUTPUT =
Output medium.

OUTPUT = *SYSOUT(...)
Output is sent to SYSOUT.

OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = *STD
Output is formatted using a standard layout that can be easily read by the user

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon “;“ (see section “Output in CSV format” on page 135).

Example

The FTAC administrator Jack John backs up the admission set and the admission profiles of the user ID STEVEN in the file STEVEN.FTAC.BKUP.

```
/EXPORT-FTAC-ENVIRONMENT␣TO-FILE=STEVEN.FTAC.BKUP,
                         USER-IDENTIFICATION=STEVEN
```

A possible short form of this command would be:

```
/EXP-FTAC-ENV␣STEVEN.FTAC.BKUP,STEVEN
```

As a conscientious FTAC administrator, Jack checks if the desired back-up is in the file STEVEN.FTAC.BKUP

```
/SHOW-FTAC-ENVIRONMENT␣FROM-FILE=STEVEN.FTAC.BKUP
```

He receives the following output:

```
                MAX. USER LEVELS              MAX. ADM LEVELS          ATTR
% USER-ID  OBS  OBR  IBS  IBR  IBP  IBF   OBS  OBR  IBS  IBR  IBP  IBF
% STEVEN     1    1    0    1    0    0     1    1    0    0    0    0
% OWNER     NAME
% STEVEN   *UMSAWARE
```

USER-ID and OWNER can be used to determine the user ID with which the admission sets and profiles defined under NAME are associated.

In addition, the maximum security levels set for each user are displayed, as in the command SHOW-FT-ADMISSION-SET. An explanation of these entries can be found in the section for this command (page 306).

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	FTC0054	No information exists which meets the specified criteria.
0	64	FTC0103	The file is not an FTAC export file or access is not permitted.
0	64	FTC0104	Access to the user ID denied or the user ID doesn’t exist.
0	64	FTC0105	Access to the file denied.
0	64	FTC0106	Access to the temporary file denied.
0	64	FTC0156	The command may only be issued by the FTAC administrator.
0	64	FTC0177	The filename entered is unknown.
0	64	FTC0180	The USER-ID entered occurs several times.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

The OPS variables of the displayed objects correspond to the variables of the commands SHOW-FT-ADMISSION-SET (see page 306) and SHOW-FT-PROFILE (see page 372).

5.30 SHOW-FT-ADMISSION-SET Display admission sets

Note on usage

User group: FTAC user and FTAC administrator

Prerequisite for using this command is the use of openFT-AC.

Functional description

You use the SHOW-FT-ADMISSION-SET command to display admission sets. You can output the following information on either SYSOUT or SYSLST:

- if the admission set is privileged (if so, then you are the FTAC administrator).
- if a password is required to use FTAC commands on this user ID. The password itself is not displayed.
- the limiting values for accessible security levels which have been set by the owner of this user ID.
- the limiting values for accessible security levels which have been pre-set by the FTAC administrator.

Format

```
SHOW-FT-ADMISSION-SET

 USER-IDENTIFICATION = *OWN / *ALL / *STD / <alphanum-name 1..8>
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
    *SYSOUT(...) / *SYSLST(...)
      |   LAYOUT = *STD / *CSV
```

Operands

USER-IDENTIFICATION =
User ID whose admission set you wish to view. FTAC users can only obtain information about their own admission set and the default admission set. The FTAC administrator can obtain information about any admission set.

USER-IDENTIFICATION = *OWN
FTAC outputs your own user ID’s admission set.

USER-IDENTIFICATION = *ALL
FTAC outputs the default admission set and the admission set of your own user ID.
For the FTAC administrator, all admission sets are output which differ from the default admission set.

USER-IDENTIFICATION = *STD
FTAC only outputs the default admission set.

USER-IDENTIFICATION = <alphanum-name 1..8>
FTAC outputs the admission set that belong to the of the user ID specified. The FTAC user can only enter his/her own user ID here. The FTAC administrator can enter any user ID.

OUTPUT =
Output medium for the information requested.

OUTPUT = <u>*SYSOUT</u>(...)
Output is sent to SYSOUT.

OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = <u>*STD</u>
Output is formatted using a standard layout that can be easily read by the user.

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon ";" (see section "Output in CSV format" on page 135).

Example

Jack John, the FTAC administrator of the Dack Bank, wants to obtain information about the admission sets in his system. He enters the command

```
/SHOW-FT-ADMISSION-SET˽USER-IDENTIFICATION=*ALL
```

```
FTSHWADS˽USER-IDENTIFICATION=*ALL
```

Short form:

```
/SHOW-FT-ADM˽*ALL
```

He receives the following output:

```
%              MAX. USER LEVELS         MAX. ADM LEVELS        ATTR
% USER-ID OBS OBR IBS IBR IBP IBF  OBS OBR IBS IBR IBP IBF
% *STD     10  10  10  10   0   0   10  10  10  10   0   0
% JACK    100 100   0   0   0*  0* 100 100   0   0   0*  0*   PRIV
% GRACE    50  50  10* 50  50  50   50  50  50  50  50  50    PW
% DANIEL    0  10   0   0   0   0   10  10   0   0   0   0    PW
% STEVEN   50 100   0  10*  0   0   50 100  10  50   0   0
```

These can be explained as follows:

The user ID of each admission set is in the column USER-ID. In this example, there is a default admission set as well as admission sets for the user IDs JACK, GRACE, DANIEL and STEVEN.

The column ATTR indicates the privileged admission set. We can see that JACK is the FTAC administrator.

The column ATTR also indicates whether an FTAC password has been defined (with PW). JACK, GRACE and DANIEL have done this to prevent others from using FTAC commands on their user ID which could be used to make modifications.

In the six columns under MAX-USER-LEVELS, the limiting values are output which the FTAC users have set for their admission sets. The six columns under MAX-ADM-LEVELS show the limiting values which the FTAC administrator has set. The smaller of the two values indicates up to which security level the owner of the admission set may use each basic function. The basic functions are abbreviated in the output as follows:

OBS = **O**UT**B**OUND-**S**END

OBR = **O**UT**B**OUND-**R**ECEIVE

IBS = **I**N**B**OUND-**S**END

IBR = **I**N**B**OUND-**R**ECEIVE

IBP = **I**N**B**OUND-**P**ROCESSING

IBF = **I**N**B**OUND-**F**ILEMANAGEMENT

The default admission set is configured such that it permits file transfers with systems which have the security level of 10 or lower, but does not permit any follow-up processing initiated by external sources (IBP=0). JACK may contact all available partner systems (OBS=100,OBR=100), but does not permit any file transfer accesses from outside onto his user ID (IBS=0,IBR=0,IBP=0).

The user ID GRACE is permitted to communicate with all partner systems with the security level of 50, according to the FTAC administrator's specifications. To better protect her files from strangers, GRACE has only made the function "inbound send" available to partner systems with the security level f 10 or lower.

The user ID DANIEL is heavily protected. Only files from partner systems with a maximum security level of 10 may be requested. A * after a number indicates that this value was taken from the default admission set and will change if any modifications are made to the default admission set.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	64	FTC0052	The information output was interrupted.
0	64	FTC0152	The user ID entered is not the user's own ID.
0	64	FTC0181	The FT profile name entered occurs several times.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section "Command return codes" on page 133

OPS variables

Element	Type	Output
USER-ID	String	
USER-LEV	Struct	
.MAX-OBS	Integer	
.MAX-OBS-STD	String	*YES / *NO
.MAX-OBR	Integer	
.MAX-OBR-STD	String	*YES / *NO
.MAX-IBS	Integer	
.MAX-IBS-STD	String	*YES / *NO
.MAX-IBR	Integer	
.MAX-IBR-STD	String	*YES / *NO
.MAX-IBP	Integer	
.MAX-IBP-STD	String	*YES / *NO

Element	**Type**	**Output**
.MAX-IBF	Integer	
.MAX-IBF-STD	String	*YES / *NO
ADM-LEV	Struct	
.MAX-OBS	Integer	
.MAX-OBS-STD	String	*YES / *NO
.MAX-OBR	Integer	
.MAX-OBR-STD	String	*YES / *NO
.MAX-IBS	Integer	
.MAX-IBS-STD	String	*YES / *NO
.MAX-IBR	Integer	
.MAX-IBR-STD	String	*YES / *NO
.MAX-IBP	Integer	
.MAX-IBP-STD	String	*YES / *NO
PRIV	String	*YES / *NO
.MAX-IBF	Integer	
.MAX-IBF-STD	String	*YES / *NO
PASSWORD	String	*YES / *NO

5.31 SHOW-FT-KEY
Show properties of RSA keys

Note on usage

User group: FT administrator

Alias name: FTSHWKEY

Functional description

You can use the SHOW-FT-KEY command to output the properties of RSA keys. You can display the RSA keys of your own instance as well as the RSA keys of partners.

Format

```
SHOW-FT-KEY / FTSHWKEY

 SELECT = *ALL / *OWN / *PARAMETERS (...)

   *PARAMETERS(...)
        PARTNER-NAME = *ALL / <name 1..8>
       ,EXPIRATION-DATE = *NOT-SPECIFIED / *NONE / *EXCEEDED / *UNTIL(DATE = <date 8..10>) /
               *WITHIN(DAYS = <integer 1..1000>)

,OUTPUT = *SYSOUT(...) / *SYSLST(...)

   *SYSOUT(...) / *SYSLST(...)
         LAYOUT = *STD / *CSV
```

Operands

SELECT =
Selects which keys are to be displayed.

SELECT = *ALL
Displays the keys of your own instance and the installed keys of all the partner systems.

SELECT = *OWN
Displays the keys of your own instance.

SELECT = *PARAMETERS(...)
Specifies selection criteria for the keys which are to be displayed.

PARTNER-NAME =
Partner whose key is to be displayed.

PARTNER-NAME = *ALL
Displays the installed keys of all partners.

PARTNER-NAME = <name 1..8>
Name of the partner whose key is to be displayed.

EXPIRATION-DATE =
Selects keys on the basis of their expiration date.

EXPIRATION-DATE = *NOT-SPECIFIED
The keys of the partners are displayed irrespective of their expiration date.

EXPIRATION-DATE = *NONE
Displays all partner keys that do not have an expiration date.

EXPIRATION-DATE = *EXCEEDED
Displays all partner keys that have already expired.

EXPIRATION-DATE = *UNTIL(...)
Displays all partner keys that will become invalid by a particular date.

DATE=<date 8...10>
Date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 2012-03-31 or 12-03-31 for March 31, 2012, by which date the keys will become invalid. The time on the specified day is 00:00 local time.

EXPIRATION-DATE = *WITHIN(...)
Displays all partner keys that will expire within the specified number of days.

DAYS = <integer 1...1000>
Number of days within which the keys will become invalid. The time on the last day of the period is 00:00 local time.

OUTPUT =
Output medium for the requested information.

OUTPUT = *SYSOUT(...)
Output is written to SYSOUT.

OUTPUT = *SYSLST(...)
Output is written to SYSLST.

LAYOUT = *STD
Output takes place in a format which is easy for the user to read.

LAYOUT = *CSV
Output takes place in **C**haracter **S**eparated **V**alues format. This is a table-type format which is widely used parrticularly in the PC environment and in which the individual fields are separated by a semicolon “;“ (see page 400).

OPS variables

The following table shows the OPS variables of the SHOW-FT-KEYS command.

Element	**Type**	**Output**
REF	Integer	Value
IDENTIFICATION	String	Value / *OWN
PARTNER-NAME	String	Value / *OWN
CRE-DATE	String	yyyy-mm-dd
EXP-DATE	String	yyyy-mm-dd / *NONE
EXPIRED	String	*YES / *NO
KEY-LENGTH	Integer	Value
AUTH-LEV	Integer	Value

Example

```
/SHOW-FT-KEY
CRE-DATE   EXP-DATE   KEY-LEN KEY-REF   AUTHL  PARTNER IDENTIFICATION
2011-12-31            768     2         2
2011-12-31            1024    2         2
2011-12-31            2048    2         2
2012-01-31            1024    3         2
2012-02-29            2048    4         2
2011-03-28 2012-12-24 2048    7         2      MYOWN   MYOWNID.DOMAIN.NET
2011-07-12 EXPIRED    768     12        2      PC17QD  PC17QD.DOMAIN.NET
2010-05-14            1024    1036      1      PC27ABC PC27ABC.DOMAIN.NET
```

Explanation:

CRE-DATE
Date on which the key was generated.

EXP-DATE
Date on which the key expires. The time on the specified day is 00:00 local time. EXPIRED means that the key has already expired.

If there is no specification here then there is no expiration date.

KEY-LEN
Key length in bits: 768, 1024 or 2048

KEY-REF
Key reference

AUTHL Authentication level: 1 or 2

PARTNER
Partner’s name des Partners. This field is left empty for keys belonging to your own instance.

IDENTIFICATION
Partner’s instance ID. This field is left empty for keys belonging to your own instance.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error
88	32	CMD0221	Error during OPS generation
89	32	CMD0221	Error in key file
35	64	FTR1035	Command only permissible for FT administrator
76	64	FTR1076	Selected key file not found

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.32 SHOW-FT-LOGGING-RECORDS Display log records and offline log files

Note on usage

User group: FT user, FT administrator and FTAC administrator

Alias name: FTSHWLOG

Functional description

With the SHOW-FT-LOGGING-RECORDS command, you can obtain information on all FT requests logged by openFT. An important prerequisite is that the FT administrator has switched on the FT logging function. The logging records are marked as FT or FTAC or ADM, enabling you to identify the type of logging record.

SHOW-FT-LOGGING-RECORDS also enables the name of the current log file and the names of the offline log files to be displayed.

FT logging

The FT user can view all log records which relate to his/her user ID. The FT administrator can display all the FT log records in the system.

If no options are specified, openFT outputs the most recent log record. When requested, openFT outputs all the log records which correspond to the selection criterion defined in the command.

Command execution may take several minutes, depending on the size of the log file! The output can be interrupted using the K2 key.

There are three types of output: short output and long output and CSV format.

FTAC logging

With FTAC functionality, SHOW-FT-LOGGING-RECORDS can be used to display the FTAC log records. The FT user can view all FT log records, of which he/she is the owner. FT and FTAC administrators may view all FT and FTAC log records.

If the access check was positive and openFT accepted the request, a second logging record is created in openFT, indicating whether the request was completed successfully, and if not, why it was terminated.

A precise description of output can be found starting on page 328.

ADM logging

If your openFT instance is administered via a remote administration server or if you administer other instances yourself using EXECUTE-REMOTE-FTADM-CMD, ADM log records are written (assuming that the appropriate logging settings have been made). You can also view these log records.

Format

(part 1 of 2)

```
SHOW-FT-LOGGING-RECORDS / FTSHWLOG

SELECT = *OWN / *ALL / *PARAMETERS(...)
  *PARAMETERS(...)
      LOGGING-ID = *ALL / <alphanum-name 1..12> / *INTERVAL(...)
        *INTERVAL(...)
            FROM = 1 / <alphanum-name 1..12>
           ,TO = *HIGHEST-EXISTING / <alphanum-name 1..12>
     ,OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
     ,CREATION-TIME = *INTERVAL(...) / *DAYS(...)
        *INTERVAL(...)
            FROM = 1970-01-01(...) / <date 8..10>(...)
              <date 8..10>(...)
                  TIME = 00:00 / <time 1..8>
           ,TO = *TOMORROW(...) / *TODAY(...) / <date 8..10>(...)
              <date 8..10>(...)
                  TIME = 00:00 / <time 1..8>
        *DAYS(...)
            NUMBER = <integer 1..1000>
     ,RECORD-TYPE = *ALL / *PARAMETERS(...)
        *PARAMETERS(...)
            FT = *TRANSFER-FILE / *NONE / list-poss(1): *TRANSFER-FILE
           ,FTAC = (*TRANSFER-FILE, *READ-FILE-ATTRIBUTES, *DELETE-FILE,
                   *CREATE-FILE, *MODIFY-FILE-ATTRIBUTES,
                   *READ-DIRECTORY, *MOVE-FILE, *CREATE-DIRECTORY,
                   *DELETE-DIRECTORY, *MODIFY-DIRECTORY. *LOGIN) / *NONE /
                   list-poss(11): *TRANSFER-FILE / *READ-FILE-ATTRIBUTES / *DELETE-FILE /
                   *CREATE-FILE / *MODIFY-FILE-ATTRIBUTES / *READ-DIRECTORY /
                   *MOVE-FILE / *CREATE-DIRECTORY / *DELETE-DIRECTORY /
                   *MODIFY-DIRECTORY / *LOGIN
           ,ADM = *ADMINISTRATION / *NONE / list-poss(1): *ADMINISTRATION
     ,INITIATOR = (*LOCAL, *REMOTE) / list-poss(2): *LOCAL / *REMOTE
     ,PARTNER = *ALL / <text 1..200 with-low>
     ,FILE-NAME = *ALL / <filename 1..54> / <filename-prefix 2..53> /
                <c-string 1..512 with-low> / *DIRECTORY(...) / *POSIX(NAME=<posix-pathname 1..510>)
        *DIRECTORY(...)
            NAME = *ALL / <partial-filename 1..53> / <c-string 1..512 with-low>
     ,REASON-CODE = *ALL / *FAILURE / <text 1..4>
```

(part 2 of 2)

```
          ,ROUTING-INFO = *ALL / <text 1..200 with-low>
          ,TRANSFER-ID = *ALL / <integer 1.. 2147483647>
          ,GLOBAL-REQUEST-ID = *ALL / <alphanum-name 1..10>
          ,LOGGING-FILE = *CURRENT / <filename 1..54> /  *ACTIVE-AT(...)
             *ACTIVE-AT(...)
                 DATE = <date 8..10>
                 ,TIME = 00:00 / <time 1..8>
          ,PREVIOUS-FILES = *STD / <integer 0..3>
,NUMBER = 1 / *ALL / <integer 1..99999999> / *POLLING(...)
   *POLLING(...)
          INTERVAL = 1 / <integer 1..600>
          ,NUMBER = *UNLIMITED / <integer 1..3600>
,INFORMATION = *STD / *ALL / *LOGGING-FILES
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
   *SYSOUT(...) / *SYSLST(...)
          LAYOUT = *STD / *CSV
```

Operands

SELECT =
Selects a group of logging records.

SELECT = *OWN
Selects logging records under the user’s own login.

SELECT = *ALL
Displays all users’ logging records to the administrator.

SELECT = *PARAMETERS(...)

LOGGING-ID =
Number of the logging record.

LOGGING-ID = *ALL
The number of the logging record is not a selection criterion.

LOGGING-ID = <alphanum-name 1..12>
Number of the logging record to be output. The value range for the logging ID is from 1 through 999999999999.

LOGGING-ID = *INTERVAL(...)
Range of logging records to be output.

FROM = <alphanum-name 1..12>
First logging record to be output. The value range for the logging ID is from 1 through 999999999999.

TO = *HIGHEST-EXISTING / <alphanum-name 1..12>
Last logging record to be output. The value range for the logging ID is from 1 through 999999999999.

OWNER-IDENTIFICATION =
User ID whose logging records are to be displayed.

OWNER-IDENTIFICATION = *OWN
Logging records of your user ID are displayed.

OWNER-IDENTIFICATION = *ALL
The logging records of all user IDs are displayed. The FT or FTAC administrator can thus display the FT logging records of any user ID.

OWNER-IDENTIFICATION = <name 1..8>
Any user ID whose logging records should be displayed.

CREATION-TIME =
The range of the logging records to be output, selected by their date or time of creation.

CREATION-TIME = *INTERVAL(...)
The range is specified as a time interval using the date and/or time.

FROM = 1970-01-01(...) / <date 8..10>(...)
Date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 20012-08-18 or 12-08-18 for 18 August, 2012. openFT then displays all logging records written after the specified date and time.

TIME = 00:00 / <time 1..8>
Time for the day specified with CREATION-TIME. openFT displays all logging records written after the specified time. The time is entered in the format *hh:mm:ss*, e.g. 14:30:10.

TO = *TOMORROW / *TODAY(...) / <date 8..10>(...)
Creation date up to which the log records are to be displayed.

TO = *TOMORROW
Outputs all log records which were created by the time of the command output.

TO = *TODAY
When CREATION-TIME is used to explicitly specify a time, all log records which were written up to this time are displayed. If no time was specified, openFT displays all log records which were written up to and including at midnight on the previous day.

TO=<date 8..10>(...)
Date in the format *yyyy-mm-dd* or *yy-mm-dd*, e.g. 20012-08-18 or 12-08-18 for 18 August, 2012. openFT then displays all logging records up to the specified time.

TIME = 00:00 / <time 1..8>
Time for the day specified with CREATION-TIME. openFT displays all logging records written up to the specified time. The time is entered in the format *hh:mm:ss*, e.g. 14:30:10.

CREATION-TIME = *DAYS(NUMBER=<integer 1..1000>)
This field is specified in number of days. All logging sets that were created in the last n calendar days, including today, are output.

RECORD-TYPE =
Type of logging record to be displayed.

RECORD-TYPE = *ALL
The record type is not a selection criterion.

RECORD-TYPE = *PARAMETERS(...)
Type of the logging record.

FT = *TRANSFER-FILE / *NONE / list-poss(1): *TRANSFER-FILE
Specifies whether or not the FT logging records are to be displayed.

FTAC =
(*TRANSFER-FILE, *READ-FILE-ATTRIBUTES, *DELETE-FILE, *CREATE-FILE, *MODIFY-FILE-ATTRIBUTES, *READ-DIRECTORY, *MOVE-FILE, *CREATE-DIRECTORY, *DELETE-DIRECTORY, *MODIFY-DIRECTORY, *LOGIN) / *NONE / list-poss(11): *TRANSFER-FILE / *READ-FILE-ATTRIBUTES / *DELETE-FILE / *CREATE-FILE / *MODIFY-FILE-ATTRIBUTES / *READ-DIRECTORY / *MOVE-FILE / *CREATE-DIRECTORY / *MODIFY-DIRECTORY / *DELETE-DIRECTORY / *LOGIN
Specifies whether or not FTAC logging records are to be displayed. If they are to be displayed, the FT function for which the FTAC logging records are to be displayed can also be specified. The following values are possible:

*TRANSFER-FILE
All logging records for the function “Transfer files” are displayed.

*READ-FILE-ATTRIBUTES
All logging records for the function “Read file attributes” are displayed.

*DELETE-FILE
All logging records for the function “Delete files” are displayed.

*CREATE-FILE
All logging records for the function “Create files” are displayed.

*MODIFY-FILE-ATTRIBUTES
All logging records for the function “Modify file attributes” are displayed.

*READ-DIRECTORY
All logging records for the function “Read file directory” are displayed.

*MOVE-FILE
All logging records for the function “Copy and delete files” are displayed.

*CREATE-DIRECTORY
All logging records for the function “Create directory” are displayed.

*DELETE-DIRECTORY
All logging records for the function “Delete directory” are displayed.

*MODIFY-DIRECTORY
All logging records for the function “Modify directory” are displayed.

*LOGIN
All logging records for the function “Inbound FTP access” are displayed. Log records of the type *LOGIN are only written in the case of an incorrect transfer admission.

ADM = <u>*ADMINISTRATION</u> / *NONE / list-poss(1): *ADMINISTRATION
Specifies whether ADM log records are output.

ADM = <u>*ADMINISTRATION</u>
ADM log records are output.

ADM = *NONE
No ADM log records are output.

INITIATOR =
Logging records according to the initiator.

INITIATOR = (<u>*LOCAL,*REMOTE</u>)
The initiator is not a selection criterion.

INITIATOR = *LOCAL
Only those logging records that belong to requests issued locally are displayed.

INITIATOR = *REMOTE
Only those logging records belonging to requests made from a remote system are displayed.

PARTNER =
The partner system.

PARTNER = <u>*ALL</u>
The partner system is not a selection criterion.

PARTNER = <text 1..200 with-low>
Name or address of the partner system for which the logging records are to be displayed. For more information on address specifications, see section “Defining partner properties” on page 44.

For the partner name, you can also use the wildcard symbols '*' (asterisk) and '?' (question mark). ’*’ stands for any string and ’?’ stands for any single character. The asterisk may not, however, be in first place. You can enter '?*' instead.

FILE-NAME =
File name.

FILE-NAME = *ALL
The file name is not a selection criterion.

FILE-NAME = <filename 1..54> / <c-string 1..512 with-low> / *POSIX(NAME = <posix-pathname 1..510>)
Fully qualified name of the files for which you wish to view the logging records.

FILE-NAME = <filename-prefix 2..53>
Partially qualified name of the files for which you want to view the logging records.

FILE-NAME = *DIRECTORY(...)
Name of the directory.

> ***DIRECTORY(...)**
> Here you specify the directory in the same format as used on the partner computer in one of the openFT user commands CREATE-/MODIFY-/DELETE-REMOTE-DIR or SHOW-REMOTE-FILE-ATTRIBUTES (see User Guide).
>
> > **NAME = *ALL**
> > The directory is not a selection criterion
> >
> > **NAME = <partial-filename 1..53> / <c-string 1..512 with-low>**
> > Name of the directory.
> > In BS2000, directories are represented by partially qualified file names in DVS.

REASON-CODE =
Selection by the reason code of the logging records.

REASON-CODE = *ALL
The reason code is not a selection criterion; all records are output.

REASON-CODE = *FAILURE
All logging records with error codes are output.

REASON-CODE = <text 1..4>
Logging records to be output by the error codes. Leading zeros can be omitted (e.g. 14 for FTR0014).

ROUTING-INFO = *ALL / <text 1..200 with-low>
Selects the ADM log records on the basis of the routing information. The routing information describes the administered instance in the case of remote administration requests issued locally.

ROUTING-INFO = *ALL
The routing information is not used as a selection criterion.

ROUTING-INFO = <text 1..200 with-low>
Routing information for which the ADM log records are to be output.

TRANSFER-ID =
Selection on the basis of the request ID.

TRANSFER-ID = *ALL
The request ID is not used as a selection criterion.

TRANSFER-ID = <integer 1..2147483647>
Only outputs log records for the specified request ID.

GLOBAL-REQUEST-ID = *ALL / <alphanum-name 1..10>
Selects the log records on the basis of the global request ID.

GLOBAL-REQUEST-ID = *ALL
The global request identification is not a search criterion.

GLOBAL-REQUEST-ID = <alphanum-name 1..10>
Outputs log records for the specified global request identification. The global request identification is relevant only for inbound requests of openFT and FTAM partners. It is assigned by the initiator of the request (transfer ID) and transferred to the local system.

LOGGING-FILE =
Selects the log file whose logging records or name are to be output. This means that you can also view offline log records.

LOGGING-FILE = *CURRENT
The current log file is selected.

LOGGING-FILE = <filename 1..54>
Specifies the name of the log file which is to be searched. If you specify a value > 0 in the PREVIOUS-FILES operand, further, older offline log files are also searched (if any exist).

LOGGING-FILE = *ACTIVE-AT(...)
Selects the log file using its creation time (local time). The log file which was created on or before the specified time is selected. If more than one log file matches the specified time, the most recent of these log files is selected. If you specify a value > 0 in the PREVIOUS-FILES operand, further, older offline log files are also searched (if any exist).

DATE = <date 8..10>
Creation date in the format *yyyy-mm-dd* or *yy-mm-dd*, z.B. 2012-01-31 or 12-01-31 for Januray 31, 2012.

TIME = 00:00 / <time 1..8>
Creation time on the date specified with DATE. You specify the time in the format *hh:mm:ss*, e,.g. 14:30:10.

PREVIOUS-FILES =
Specifies the number of preceding offline log files that are to be selected in addition to the current file or the file specified with LOGGING-FILE.

PREVIOUS-FILES = *STD
The effect depends on the specification in the INFORMATION operand:

– INFORMATION = *STD (default value) or *ALL: The current lo file or the log file specified with LOGGING-FILE is searched for log records.

– INFORMATION = *LOGGING-FILES: The names of all log files are output (maximum of 1024).

PREVIOUS-FILES = <0..3>
Specifies the number of preceding offline log files (0 to 3) that are to be searched in addition to the current file or the file specified with LOGGING-FILE or whose names are to be output.

NUMBER =
Maximum number of log records or polling intervals for outputting log records.

NUMBER = 1 / <integer 1..99999999>
The maximum number of logging records that are to be displayed. The default value is 1.

NUMBER = *ALL
All logging records are displayed.

NUMBER = *POLLING(...)
Specifies that the output of log records will be repeated at regular intervals. You can define the polling interval and the number of repetitions. Irrespective of the specifications in INTERVAL and NUMBER, the most recent log record which exists is always output first.

INTERVAL = 1 / <integer 1...600>
Polling interval in seconds. On each repetition, all the new log records are filtered in accordance with the specified selection criteria and the detected records are output. By default the output is repeated every second.

NUMBER =
Number of repetitions.

NUMBER = *UNLIMITED
The output is repeated without restriction. You can, for example, cancel the output using key K2.

NUMBER = <integer 1..3600>
Specifies the number of reperitions.

NUMBER = *POLLING may not be combined with the following specifications:
- LOGGING-FILE = <filename ..>
- LOGGING-FILE = *ACTIVE-AT(...)
- INFORMATION = *LOGGING-FILES
- TRANSFER-ID = <integer 1..2147483647>
- GLOBAL-REQUEST-ID = <alphanum-name 1..10>
- LOGGING-ID = <alphanum-name 1..12> / *INTERVAL(...)
- CREATION-TIME = *INTERVAL(...) / *DAYS(...)
- PREVIOUS-FILES = <integer 0..3>

INFORMATION =
Scope of the requested information.

INFORMATION = *STD
The logging records are displayed in a standard format (see page 326).

INFORMATION = *ALL
The logging records are displayed in a detailed format (see page 328).

INFORMATION = *LOGGING-FILES
Outputs only the names of the log file(s).

INFORMATION = *LOGGING-FILES can only be combined with the following parameters:
- LOGGING-FILE in SELECT=*PARAMETERS(…)
- PREIOUS-FILES in SELECT=*PARAMETERS(…)
- OUTPUT

OUTPUT =
Output medium.

OUTPUT = *SYSOUT(...)
Output is sent to SYSOUT.OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = *STD
Output is formatted using a standard layout that can be easily read by the user.

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon “;“ (see page 135).

5.32.1 Description of the short output

Short output form of FT logging records (example)

```
/SHOW-FT-LOGGING-RECORDS NUMBER = 2
```

```
%TYP LOGG-ID  TIME     RC    PARTNER  INITIATOR INIT USER-ADM FILENAME
%2012-02-26
%T       5333 14:18:24 0014 <G133H301 FT2V292   1TCL FT2V292  TEST2
%T       5284 14:08:12 0000 >G133H301 FT2V292   1TCL FT2V292  TEST1
```

Short output format for ADM log records (examples)

ADM log for a remote administration request that has been issued locally and its corresponding FTAC log record:

```
%TYP LOGG-ID  TIME     RC    PARTNER  INITIATOR INIT USER-ADM FILENAME
%2012-02-26
%T       5333 14:18:24 0014 <G133H301 FT2V292   1TCL FT2V292  TEST2
%T       5284 14:08:12 0000 >G133H301 FT2V292   1TCL FT2V292  TEST1
```

ADM log record on the administered openFT instance:

```
/SHOW-FT-LOGGING-RECORDS NUMBER=1
```

```
%TYP LOGG-ID TIME    RC    PARTNER  INITIATOR INIT USER-ADM FILENAME
%2012-06-27
%A     9006 11:32:51 0000 >ftadm:/* *REMOTE        ftadmin
```

Explanation

Not all values are displayed for all log record types and request types.

Name	Explanation
TYP (column 1)	Specifies if it is an FT or FTAC or ADM or FTP log record. T indicates the FT logging record, C indicates the FTAC logging record, A indicates the ADM logging record, P indicates the FTP logging record written by the FTP server from the product „interNet Services in BS2000/OSD“.

Name	Explanation	
TYP (columns 2-3)	Definition of FT function:	
	␣	transfer file
	V	transfer file and delete send file (only inbound possible)
	A	read file attributes
	D	delete file
	C	create file
	M	modify file attributes
	R	read directory
	CD	create director
	MD	modify directory
	DD	delete directory
	L	login (inbound FTP access)
LOGG-ID	Number of the log record (up to twelve digits)	
TIME	Time when the logging record was written	
RC	Reason Code. Indicates if a request was successfully executed, or if not, why it was rejected or terminated. If an FT request is rejected for “FTAC reasons” (e.g. 0014), the exact reason behind the termination can be found in the FTAC logging record of the system that rejected the request. Further information on the reason code can be obtained using the BS2000 command HELP-MSG-INFORMATION (FTCxxxx for FTAC type or FTRxxxx for FT type).	
PARTNER	Provides information about the partner system. The output in the case of named partners consists of the symbolic name, and in the case of dynamic partners of the address (up to 8 characters; if the address is longer, the last character is an'*'). The partner system is prefixed by an identifier from which you can determine the request direction.	
	>	The request direction is to the partner system. This direction is specified for a – send request, i.e. the data is transferred to the partner – request to view remote file attributes – request to view remote directories
	<	The request direction is to the local system. This direction is specified for a – receive request, i.e.the data is transferred to the local system – request to modify remote file attributes[1] – request to delete remote files
INITIATOR	Initiator (user ID) in the case of requests issued locally issued; if initiative is from remote system: *REMOTE	

Name	Explanation
INIT	TSN from which the request came. If the INITIATOR was *REMOTE, the field is empty.
USER-ADM	User ID in the local system used by the requests
FILENAME	Filename resp. pre-processing or post-processing in the local system. In the case of ADM logging records, this field is empty.

[1] When modifying the access rights of a file from an FTAM partner system, two logging records are written. In this case, no direction is specified before the PARTNER output.

5.32.2 Description of the long output

Long output form outbound (example)

```
%LOGGING-ID  = 38735     RC      = 0000       TIME     = 2012-07-11 13:58:21
%   TRANS    = TO        REC-TYPE= FT         FUNCTION = TRANSFER-FILE
%   PROFILE  =           PCMD    = NONE       STARTTIME= 2012-07-11 13:58:21
%   TRANS-ID = 721206    WRITE   = REPLACE    REQUESTED= 2012-07-11 13:58:21
%   TRANSFER =        0 kB                    CCS-NAME =
%   SEC-OPTS = ENCR+DICHK, RSA-1024 / AES-256
%   INITIATOR= TSOS                           INITSN   = 83VV
%   USER-ADM = TSOS
%   PARTNER  = LINUX01
%   FILENAME = $USER1.FILE.TEST

%LOGGING-ID  = 38734     RC      = 0000       TIME     = 2012-07-11 13:58:21
%   TRANS    = TO        REC-TYPE= FTAC       FUNCTION = TRANSFER-FILE
%   PROFILE  =           PRIV    =
%   INITIATOR= TSOS                           INITSN   = 83VV
%   USER-ADM = TSOS
%   PARTNER  = LINUX01
%   FILENAME = $USER1.FILE.TEST
```

Long output form inbound (example)

```
LOGGING-ID   = 38733     RC       = 0000        TIME     = 2012-07-11 13:49:44
%   TRANS    = FROM      REC-TYPE= FT          FUNCTION = TRANSFER-FILE
%   PROFILE  =           PCMD     = NONE        STARTTIME= 2012-07-11 13:49:44
%   TRANS-ID = 721204    WRITE    = REPLACE     STORETIME= 2012-07-11 13:49:44
%   TRANSFER =         1 kB                     CCS-NAME =
%                                               CHG-DATE = SAME
%   SEC-OPTS = ENCR+DICHK+DENCR+DDICHK, RSA-1024 / AES-256
%   INITIATOR= *REMOTE                          GLOB-ID  = 66277
%   USER-ADM = USER1
%   PARTNER  = LINUX01
%   FILENAME = TEST1
```

```
LOGGING-ID   = 38732     RC       = 0000        TIME     = 2012-07-11 13:49:44
%   TRANS    = FROM      REC-TYPE= FTAC        FUNCTION = TRANSFER-FILE
%   PROFILE  = PROF1     PRIV     = NO
%   INITIATOR= *REMOTE                          GLOB-ID  = 66277
%   USER-ADM = USER1
%   PARTNER  = LINUX01
%   FILENAME = TEST1
```

Long output format for an ADM log record (example)

```
LOGGING-ID  = 45067     RC       = 0000        TIME     = 2012-08-29 09:43:57
   TRANS    = TO        REC-TYPE= ADM         FUNCTION = REM-ADMIN
   TRANS-ID = 156730    PROFILE = Profil04
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= *REMOTE                          GLOB-ID  = 192929
   USER-ADM = FTADMIN8
   PARTNER  = REMADMIN
   ADM-CMD  = SHOW-FT-LOGGING-RECORDS
   ADMIN-ID =
   ROUTING  =
```

Explanation of long output form (column-wise)

Name	Explanation	
LOGGING-ID	Number of the log record (up to twelve digits)	
TRANS	Transfer direction:	
	TO	The request direction is to the partner system. This direction is specified for a – send request, i.e. the data is transferred to the partner. – request to view remote file attributes – request to view remote directories
	FROM	The request direction is to the local system (inbound). This direction is specified for a – receive request, i.e. the data are transferred to the local system – request to modify remote file attributes [1] – request to delete remote files
	BOTH	File management request with two-way data transfer.
PROFILE	Name of the profile to be used for the transfer (empty in the FT logging record)	
TRANS-ID	Transfer ID number	
TRANSFER	Amount of data transferred	
PROTECT	Specifies whether the protection attributes are transferred. Is only output if this option was specified in the transfer request.	
	SAME	The protection attributes of the file were transferred.

<table>
<tr><th>Name</th><th colspan="2">Explanation</th></tr>
<tr><td rowspan="11">SEC-OPTS</td><td colspan="2">Security options and encryption algorithms used. This line is only output if at least one of the options is used.</td></tr>
<tr><td>ENCR</td><td>Encryption of the request queue</td></tr>
<tr><td>DICHK</td><td>Data integrity check of the request queue</td></tr>
<tr><td>DENCR</td><td>Encryption of data content during the transfer</td></tr>
<tr><td>DDICHK</td><td>Data integrity check of the file data to be transferred</td></tr>
<tr><td>LAUTH</td><td>Authentication of the local system on a partner (authentication level 1)</td></tr>
<tr><td>LAUTH2</td><td>Authentication of the local system on a partner (autehtication level 2)</td></tr>
<tr><td>RAUTH</td><td>Authentication of the partner on a local system (authentication level 1)</td></tr>
<tr><td>RAUTH2</td><td>Authentication of the partner on a local system (authentication level 2)</td></tr>
<tr><td>RSA-nnnn</td><td>Length of the RSA key</td></tr>
<tr><td>DES /
AES-128 /
AES-256</td><td>Encryption algorithm used</td></tr>
<tr><td>INITIATOR</td><td colspan="2">Initiator (user ID) in the case of requests issued locally issued;
if initiative is from remote system: *REMOTE</td></tr>
<tr><td>USER-ADM</td><td colspan="2">User ID in the local system used by the requests</td></tr>
<tr><td>PARTNER</td><td colspan="2">Provides information about the partner system. The output includes the symbolic name under which the system administrator has entered the partner system in the partner list. If dynamic partners are admitted, the partner system can be output as partner address.</td></tr>
<tr><td>FILENAME</td><td colspan="2">Filename resp. pre-processing or post-processing in local system.</td></tr>
<tr><td>ADM-CMD</td><td colspan="2">Only output for an ADM log record:
Administration command without parameters</td></tr>
<tr><td>ADMIN-ID</td><td colspan="2">Only output for an ADM log record:
Remains always empty in BS2000 because only relevant on the remote adminsitration server</td></tr>
<tr><td>ROUTING</td><td colspan="2">Only output for an ADM log record::
Routing information on the openFT instance to be administered</td></tr>
</table>

Name	**Explanation**	
RC	Reason-Code. Indicates if a request was successfully executed, or if not, why it was rejected or terminated. If an FT request is rejected for “FTAC reasons” (e.g. 2169), the exact reason behind the termination can be found in the FTAC logging record of the system that rejected the request. Further information on the reason code can be obtained using the BS2000 command HELP-MSG-INFORMATION (FTCxxxx for FTAC type or FTRxxxx for FT type).	
REC-TYPE	Specifies if this is an FT or FTAC or ADM logging record.	
PCMD	Status of follow-up processing:	
	NONE	No follow-up processing defined.
	STARTED	Follow-up processing was started.
	NOT-STARTED	Follow-up could not be started.
PRIV	specifies whether the admission profile is privileged.	
WRITE	Write rules:	
	NEW	A new file is created. If a file with the same name already exists, the transfer will be aborted.
	EXT	An existing file is extended and stored as new.
	REPLACE	An existing file is extended.
TIME	Time when the logging record was written	
FUNCTION	Definition of FT function:	
	– TRANSFER-FILE: transfer file – MOVE-FILE: transfer file and delete send file (only inbound possible) – READ-FILE-ATTRIBUTES: read file attributes – DELETE-FILE: delete file – CREATE-FILE: create new file – MODIFY-FILE-ATTRIBUTES: modify file attributes – READ-DIRECTORY: read directory – CREATE-DIRECTORY: create directory – MODIFY-DIRECTORY: modify directory – DELETE-DIRECTORY: delete directory – LOGIN: inbound FTP access – REM-ADMIN: remote administrator	
STARTTIME	Time request was started	
STORETIME	Time request was accepted (inbound)	
REQUESTED	Time request was accepted (outbound)	
CCS-NAME	Name of the character set, used for code conversion as necessary.	
CHG-DATE	Specifies whether the change date of the send file is taken over for the receive file.	
	SAME	The change date of the send file is take over.

Name	Explanation
INITSN	TSN from which the request came, entered only in the case of outbound requests.
GLOB-ID	Global request identification, displayed only in the case of inbound requests from openFT and FTAM partners (INITIATOR=REMOTE). This corresponds to the request identification (=TRANSFER-ID) on the initiator system.

[1] When modifying the access rights of a file from an FTAM partner system, two logging records are written. In this case, no direction is specified before the PARTNER output.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	No log records available for the selection criteria.
33	32	CMD0221	Request rejected. Internal error.
36	32	CMD0221	Request rejected. Request data inconsistent.
83	32	CMD0221	Internal error.
88	32	CMD0221	Error during OPS generation.
36	64	FTR1036	User not authorized for other user IDs.
2	0	FTR2225	Information output cancelled.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

The following table shows the OPS variables for the command SHOW-FT-LOGGING-RECORDS with the operand INF=*ALL. The underlined values are valid for the output with the operand INF=*STD. The output for INF = *LOGGING-FILES has its own format, see page 335.

Depending on the type of log record, not all elements are output.

Element	Type	Output
LOG-ID	Integer	
REASON-CODE [1]	Integer	
LOG	Struct	
.DATE	String	yyyy-mm-dd
.TIME	String	hh:mm:ss
INIT-USER-ID	String	USER-ID of request initiator / *REM
INIT-TSN [2]	String	TSN of request initiator
PARTNER-NAME	String	

Element	Type	Output
TRANS-DIRECT	String	*TO-PARTNER / *FROM-PARTNER / *NOT-SPECIFIED
REC-TYPE	String	*FT / *FTAC
FUNC	String	*TRANS-FILE / *READ-FILE-ATTR / *DEL-FILE / *CRE-FILE / *MOD-FILE-ATTR / *READ-DIR / *CRE-DIR / *MOD-DIR / *DEL-DIR / *MOVE-FILE / *LOGIN
USER-ADMIS	String	
WRITE-MODE	String	*REPL-FILE / *NEW-FILE / *EXT-FILE
RESULT-PROCESS	String	*NONE / *STARTED / *NOT-STARTED
START	Struct	
.DATE	String	yyyy-mm-dd
.TIME	String	hh:mm:ss
TRANS-ID	Integer	
STORE	Struct	
.DATE	String	yyyy-mm-dd
.TIME	String	hh:mm:ss
BYTE-NUM	String / Integer	*NONE / Value
PRIVIL [3]	String	*NO / *YES
PROF-NAME [3]	String	
F-NAME	String	
SEC	Struct	
.PROT.ENC	String	*NO / *YES
.PROT.INT-CHECK	String	*NO / *YES
.USER-DATA.ENC	String	*NO / *YES
.USER-DATA.INT-CHECK	String	*NO / *YES
.LOC-AUTH	String	*NO / *YES
.REM-AUTH	String	*NO / *YES
.AUTH-LEV	Integer	1 / 2 / empty
RSA-KEY-LEN	Integer	
SYMM-ENC-ALG	String	*DES / *AES
PROTECTION [4]	String	*STD / *SAME
ADMINISTRATOR-ID [5]	String	Value
ADM-CMD [5]	String	Value

Element	Type	Output
ROUTING [5]	String	Value
CHANGE-DATE	String	*STD / *SAME
GLOBAL-REQ-ID	Integer	global request identification / empty

[1] The reason code is always given in decimal form. To determine the meaning of FTAC logging records using the manual, the value must be converted to hexadecimal form.

[2] For INIT-USER-ID=*REM, INIT-TSN is not assigned.

[3] Only for REC-TYPE=*FTAC and specification of a profile.

[4] Only with FT log records, not with FTAC or ADM log records

[5] Only for REC-TYPE = ADM

When you specify the INF=*LOGGING-FILES operand, only the two elements below are output:

Element	Type	Output
TIME-STAMP	String	yyyy-mm-dd hh:mm:ss
FILE-NAME	String	Wert

Example 1

The FT administrator wants to display all logging records that were created for the user ID *Meier* and logged between 01.01.2012 and 31.03.2012. If you are the owner of the User ID

```
/SHOW-FT-LOGGING-RECORDS SELECT=*PARAMETERS(OWNER-IDENTIFICATION=Meier, -
/                        CREATION-TIME=*INTERVAL(FROM=2012-01-01(00:00), -
/                           TO=2012-03-31(23:59))),NUMBER=*ALL
```

You want to see the first record of the output in detail.

```
/SHOW-FT-LOG-REC (OWN=Meier,CRE-TIME=*INTERVAL(FROM=2012-01-01(00:00),  -
/                           TO=2012-03-31(00:00))),INF=*ALL
```

Example 2

An (FT or FTAC) administrator wants to view all log records. He/She wants all the information to be output in the most compact possible form because he/she wants to back up the log records before deleting them. To do this, he/she combines the specifications for "comprehensive output" and "output in CSV format". This is achieved using the following command:

```
/SHOW-FT-LOG-REC SELECT=*ALL,NUMBER=*ALL,INF=*ALL,OUTPUT=*SYSLST(*CSV)
```

This command may take a few minutes to output comprehensive information.

Example 3

The FT or FTAC administrator wishes to display the names of the current log file and and current offline log files:

```
/SHOW-FT-LOG-REC INF=*LOGGING-FILES
% $SYSFJAM.SYSLOG.L120806.L132626
% $SYSFJAM.SYSLOG.L120806.L132615
```

5.33 SHOW-FT-MONITOR-VALUES Show monitoring data

Note on usage

User group: FT users and FT administrators

Alias: FTSHWMON

Description of the function

The SHOW-FT-MONITOR-VALUES command allows you to output the monitoring values from openFT operation on the local system. To do this, monitoring must be activated (see MODIFY-FT-OPTIONS) and openFT must be activated.

Format

```
SHOW-FT-MONITOR-VALUES / FTSHWMON
--------------------------------------------------------------------
 NAME = *STD / *ALL /<list-poss(100): alphanum-name 1..12>

,POLLING =*NONE / *PARAMETERS(...)

    *PARAMETERS(...)
       |  INTERVAL=1 /<integer 1..600>
       |  ,NUMBER=*UNLIMITED / <integer 1..3600>

,INFORMATION=*VALUES(...) / *TYPE

    *VALUES(...)
       |  DATA=*FORMATTED / *RAW

,OUTPUT= *SYSOUT(...) /  *SYSLST(...)

    *SYSOUT(...) / *SYSLST(...)
       |   LAYOUT = *STD / *CSV
```

Operands

NAME =
Specifies what monitoring values are to be output.

NAME = *STD
A predefined default set of monitoring values is output, see “Examples” on page 348.

NAME = *ALL
All monitoring values are output.

NAME = <list-poss(100): alphanum-name 1..12>
Here you can enter a list of up to 100 names of monitoring values that are to be output. The name must be one of the short names (see the table in the section "Description of the monitoring values" on page 343).

POLLING =
Specifies the interval at which the monitoring values are to be polled.

POLLING =*NONE
The monitoring values are only polled once.

POLLING =*PARAMETERS
In this structure you specify a time interval and a repetition factor for polling the monitoring values. If an error occurs during polling, further repeated output is canceled.

INTERVAL = 1
The time interval for polling the monitoring values is 1 second.

INTERVAL = <integer 1..600>
Time interval in seconds for polling the monitoring values.

NUMBER = *UNLIMITED
There is no limit to the number of times the monitoring values are polled. You terminate the command by canceling output by pressing K2.

NUMBER = <integer 1..3600>
Here you specify how often the monitoring values are to be polled.

INFORMATION =
Specifies whether the monitoring values themselves or the type of the monitoring values is to be output.

INFORMATION = *VALUES(...)
The measured value is output. You can specify whether the monitoring values are to be output in formatted form or as raw data.

DATA =*FORMATTED
The monitoring values are formatted for visual display, e.g. as throughput, maximum or average.

DATA =*RAW
Raw, unformatted data is output. Monitoring values for the duration of an action are not output.

INFORMATION = *TYPE
Outputs the type and, where applicable, the scaling factor of the monitoring value or the type of the metadata.

The scaling factor is only of significance for some monitoring values and in CSV format if *RAW is not specified. In this case, the output value must be divided by the scaling factor to get the real value. In the case of formatted data in tabular format, the scaling factor 100 specifies that the number is output to 2 decimal places.

The following output values are possible for *TYPE:

*BOOL	Boolean value
*PERCENT	Percentage
*INT	Integer number (corresponds to *INT(1))
*INT(100)	Integer value with a scaling factor of 100
*TIME	Timestamp
*STRING	Text output for the selection

OUTPUT =
Output medium.

OUTPUT = <u>*SYSOUT</u>(...)
The data is output to SYSOUT.

OUTPUT = *SYSLST(...)
The data is output to SYSLST.

LAYOUT = <u>*STD</u>
Output is formatted in a form readable by the user.
If the monitoring configuration changes (filters), a new header and a new start time for monitoring is output in standard output format.

LAYOUT = *CSV
Data is output in Character Separated Values format. This is a quasi-tabular format that is in widespread use in the field of PCs and in which the individual fields are separated by semicolons ";" (see section “Output in CSV format” on page 135).

If the monitoring configuration changes (filters), the new start time for monitoring is shown in a separate column in CSV format.

Command return codes

(SC2)	SC1	Maincode	Bedeutung
51	32	CMD0221	Internal error.
88	32	CMD0221	Error on OPS output.
1	0	FTR1039	open FT not active
59	64	FTR1059	Monitoring is not active.
2	0	FTR2225	Information output cancelled.

SC1/2 = subcode 1/2 in decimal format
For additional information refer to the section “Command return codes” on page 133.

OPS variables

The following table shows the OPS variables for the SHOW-FT-MONITOR-VALUES command, which are output with the operand NAME = *ALL. Values shown in bold are also output with the operand NAME = *STD.

Element	Type	Output
CURRENT	Struct	
.DATE	String	yyyy-mm-dd
.TIME	String	hh:mm:ss
MON-START	Struct	
.DATE	String	yyyy-mm-dd
.TIME	String	hh:mm:ss
PARTNER-SEL	Struct	
.OPENFT	String	*YES / *NO
.FTAM	String	*YES / *NO
.FTP	String	*YES / *NO
REQUEST-SEL	Struct	
.ASYNC	String	*YES / *NO
.SYNC	String	*YES / *NO
.LOCAL	String	*YES / *NO
.REMOTE	String	*YES / *NO
THROUGHPUT	Struct	
.NET-BYTES-TOTAL	String	Value
.NET-BYTES-SEND	String	Value
.NET-BYTES-RCV	String	Value
.NET-BYTES-TEXT	String	Value

Element	Type	Output
.NET-BYTES-BIN	String	Value
.DISK-TOTAL	String	Value
.DISK-SEND	String	Value
.DISK-RCV	String	Value
.DISK-TEXT	String	Value
.DISK-BIN	String	Value
.REQ-TOTAL	String	Value
.REQ-F-TRANS	String	Value
.REQ-F-MANAG	String	Value
.REQ-SUCC	String	Value
.REQ-ABORT	String	Value
.REQ-INTR	String	Value
.ADMIS-FAIL	String	Value
.FOLLOWUP	String	Value
.CONN-SUCC	String	Value
.CONN-FAIL	String	Value
.CONN-ABORT	String	Value
DURATION	Struct	
.REQ-TOTAL-OUTB	String	Value
.REQ-TOTAL-INB	String	Value
.REQ-F-TRANS-OUTB	String	Value
.REQ-F-TRANS-INB	String	Value
.REQ-F-MANAG-OUTB	String	Value
.REQ-F-MANAG-INB	String	Value
.REQ-WAIT	String	Value
.DNS-OUTB	String	Value
.DNS-INB	String	Value
.CONN-ESTABL	String	Value
.F-OPEN-OUTB	String	Value
.F-OPEN-INB	String	Value
.F-CLOS-OUTB	String	Value
.F-CLOS-INB	String	Value
.ADMIS-CHECK-OUTB	String	Value

Element	**Type**	**Output**
.ADMIS-CHECK-INB	String	Value
STATE	Struct	
.NUM-REQ-ACT-ASYN	String	Value
.NUM-REQ-ACT-SYN	String	Value
.NUM-REQ-WAIT	String	Value
.NUM-REQ-HOLD	String	Value
.NUM-REQ-SUSPEND	String	Value
.NUM-REQ-LOCK	String	Value
.NUM-REQ-FINISH	String	Value
.CONN-LIM	String	Value
.NUM-CONN-ACT	String	Value
.REQ-LIM	String	Value
.NUM-REQ-QUEUE	String	Value
.OPENFT-ACT	String	Value
.FTAM-ACT	String	Value
.FTP-ACT	String	Value
.TRACE	String	Value

5.33.1 Description of the monitoring values

The table below shows all the monitoring values output when NAME=*ALL is specified. Under NAME=, you can also specify a list of any of the parameters shown in the table.

The first two letters of the name indicate the data object that the monitoring value belongs to.

– Th = Throughput
– Du = Duration
– St = State

The second component of the name indicates the performance indicator, e.g. Netb for net bytes. In the case of monitoring values for the Throughput or Duration data object, the last 3 letters of the name indicate the types of requests from which the monitoring value originates, e.g.

– Ttl = FT Total
– Snd = FT Send requests
– Rcv = FT Receive requests
– Txt = Transfer of text files
– Bin = Transfer of binary files
– Out = FT Outbound
– Inb = FT Inbound

i If monitoring is deactivated for all partners (PARTNER-SELECTION=*NONE with MODIFY-FT-OPTIONS ...,MONITORING), only the following values are provided:

Status: StCLim, StCAct, StRqLim, StRqAct, StOftr, StFtmr, StFtpr, StTrcr

All the other values are set to 0.

Name	Meaning	Output with	Output unit	
			FORMATTED	RAW
ThNetbTtl	Throughput in net bytes: Number of bytes transferred	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThNetbSnd	Throughput in net bytes (send requests): Number of bytes transferred with send requests	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThNetbRcv	Throughput in net bytes (receive requests): Number of bytes transferred with receive requests	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThNetbTxt	Throughput in net bytes (text files): Number of bytes transferred when transferring text files	*ALL	Number of bytes per second	Bytes, accumulated

Name	Meaning	Output with	Output unit	
			FORMATTED	RAW
ThNetbBin	Throughput in net bytes (binary files): Number of bytes transferred when transferring binary files	*ALL	Number of bytes per second	Bytes, accumulated
ThDiskTtl	Throughput in disk bytes: Number of bytes read from files or written to files with transfer requests	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThDiskSnd	Throughput in disk bytes (send requests): Number of bytes read from files with send requests	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThDiskRcv	Throughput in disk bytes (receive requests): Number of bytes written to files with receive requests	*STD/ *ALL	Number of bytes per second	Bytes, accumulated
ThDiskTxt	Throughput in disk bytes (text files): Number of bytes read from text files or written to text files with transfer requests	*ALL	Number of bytes per second	Bytes, accumulated
ThDiskBin	Throughput in disk bytes (binary files): Number of bytes read from binary files or written to binary files with transfer requests	*ALL	Number of bytes per second	Bytes, accumulated
ThRqto	openFT requests: Number of openFT requests received	*STD/ *ALL	Number per second	Accumulated number
ThRqft	File transfer requests: Number of file transfer requests received	*ALL	Number per second	Accumulated number
ThRqfm	File management requests: Number of file management requests received	*ALL	Number per second	Accumulated number
ThSuct	Successful requests: Number of successfully completed openFT requests	*STD/ *ALL	Number per second	Accumulated number
ThAbrt	Aborted requests: Number of aborted openFT requests	*STD/ *ALL	Number per second	Accumulated number
ThIntr	Interrupted requests: Number of interrupted openFT requests	*STD/ *ALL	Number per second	Accumulated number
ThUsrf	Requests from non-authorized users: Number of openFT requests in which the user check was terminated with errors	*STD/ *ALL	Number per second	Accumulated number

Name	Meaning	Output with	Output unit	
			FORMATTED	RAW
ThFoll	Started follow-up processing operations: Number of follow-up processing operations started	*ALL	Number per second	Accumulated number
ThCosu	Connections established: Number of connections successfully established	*ALL	Number per second	Accumulated number
ThCofl	Failed connection attempts: Number of attempts to establish a connection that failed with errors	*STD/ *ALL	Number per second	Accumulated number
ThCobr	Disconnections: Number of disconnections as a result of connection errors	*STD/ *ALL	Number per second	Accumulated number
DuRqtlOut	Maximum outbound request duration: Maximum request duration of an outbound request	*ALL	Milliseconds [1]	-
DuRqtlInb	Maximum inbound request duration: Maximum request duration of an inbound request	*ALL	Milliseconds [1]	-
DuRqftOut	Maximum outbound transfer request duration: Maximum duration of an outbound file transfer request	*ALL	Milliseconds [1]	-
DuRqftInb	Maximum inbound transfer request duration: Maximum duration of an inbound file transfer request	*ALL	Milliseconds [1]	-
DuRqfmOut	Maximum outbound file management request duration: Maximum duration of an outbound file management request	*ALL	Milliseconds [1]	-
DuRqfmInb	Maximum inbound file management request duration: Maximum duration of an inbound file management request	*ALL	Milliseconds [1]	-
DuRqesOut	Maximum outbound request waiting time: Maximum waiting time before an outbound request is processed (for requests without a specific start time)	*ALL	Milliseconds [1]	-

Name	Meaning	Output with	Output unit	
			FORMATTED	RAW
DuDnscOut	Maximum duration of an outbound DNS request Maximum time an outbound openFT request was waiting for partner checking	*ALL	Milliseconds [1]	-
DuDnscInb	Maximum duration of an inbound DNS request Maximum time an inbound openFT request was waiting for partner checking	*ALL	Milliseconds [1]	-
DuConnOut	Maximum duration of establishment of a connection: Maximum time between requesting a connection and receiving confirmation of a connection for an outbound openFT request	*ALL	Milliseconds [1]	-
DuOpenOut	Maximum file open time (outbound): Maximum time an outbound openFT request required to open the local file	*ALL	Milliseconds [1]	-
DuOpenInb	Maximum file open time (inbound): Maximum time an inbound openFT request required to open the local file	*ALL	Milliseconds [1]	-
DuClosOut	Maximum file close time (outbound): Maximum time an outbound openFT request required to close the local file	*ALL	Milliseconds [1]	-
DuClosInb	Maximum file close time (inbound): Maximum time an inbound openFT request required to close the local file	*ALL	Milliseconds [1]	-
DuUsrcOut	Maximum user check time (outbound): Maximum time an outbound openFT request required to check the user ID and transfer admission	*ALL	Milliseconds [1]	-
DuUsrcInb	Maximum user check time (inbound): Maximum time an inbound openFT request required to check the user ID and transfer admission	*ALL	Milliseconds [1]	-
StRqas	Number of synchronous requests in the ACTIVE state	*STD/ *ALL	Average [2]	Current number
StRqaa	Number of asynchronous requests in the ACTIVE state	*STD/ *ALL	Average value [2]	Current number
StRqwt	Number of requests in the WAIT state	*STD/ *ALL	Average value [2]	Current number

Name	Meaning	Output with	Output unit	
			FORMATTED	RAW
StRqhd	Number of requests in the HOLD state	*STD/ *ALL	Average value [2]	Current number
StRqsp	Number of requests in the SUSPEND state	*STD/ *ALL	Average value [2]	Current number
StRqlk	Number of requests in the LOCKED state	*STD/ *ALL	Average value [2]	Current number
StRqfi	Number of requests in the FINISHED state	*ALL	Average value [2]	Current number
StCLim	Maximum number of connections: Upper limit for the number of connections established for asynchronous requests.	*STD/ *ALL	Value currently set	
StCAct	Number of occupied connections for asynchronous requests	*STD/ *ALL	Share of StCLim in % [3]	Current number
StRqLim	Maximum number of requests: Maximum number of asynchronous requests in request management	*STD/ *ALL	Value currently set	
StRqAct	Entries occupied in request management	*STD/ *ALL	Share of StRqLim in % [3]	Current number
StOftr	openFT protocol activated/deactivated	*STD/ *ALL	ON (activated) OFF (deactivated)	
StFtmr	FTAM protocol activated/deactivated	*STD/ *ALL	ON (activated) OFF (deactivated)	
StFtpr	FTP protocol activated/deactivated	*STD/ *ALL	ON (activated) OFF (deactivated)	
StTrcr	Trace activated/deactivated	*ALL	ON (activated) OFF (deactivated)	

[1] Maximum value during the last monitoring interval (= time elapsed since the last time the monitoring values were queried or since the start of monitoring). The minimum time interval output is 1 millisecond if a relevant measurement has been completed during the interval since the last query. A value of 0 specifies that no measurement has been made in this interval.

[2] Average value during the monitoring interval (= time elapsed since the last time the monitoring values were queried or since the start of monitoring). The format is n.mm, where n is an integer and mm are to be interpreted as decimal places.

[3] If the reference value is reduced in live operation, it is possible for the value output to lie above 100 (%) temporarily.

5.33.2 Examples

1. Monitoring values are to be output in default output format.

```
/SHOW-FT-MONITOR-VALUES
openFT(STD)   Monitoring (formatted)
MonOn=2012-02-17 15:36:12 PartnerSel=OPENFT  RequestSel=ONLY-ASYNC,ONLY-LOCAL
2012-02-17 15:40:01

 Name      Value
 ----------------
 ThNetbTtl 38728
 ThNetbSnd 38728
 ThNetbRcv 0
 ThDiskTtl 16384
 ThDiskSnd 16384
 ThDiskRcv 0
 ThRqto    1
 ThSuct    0
 ThAbrt    0
 ThIntr    0
 ThUsrf    0
 ThCofl    0
 ThCobr    0
 StRqas    0.00
 StRqaa    8.66
 StRqwt    1.66
 StRqhd    0.00
 StRqsp    0.00
 StRqlk    0.00
 StCLim    16
 StCAct    37
 StRqLim   1000
 StRqAct   1
 StOftr    ON
 StFtmr    OFF
 StFtpr    OFF
```

Explanation

The default output format begins with a header containing the following specifications:

- Name of the openFT instance and selected data format (raw or formatted)
- Monitoring start time and partner and request selection
- Current timestamp

This is followed by the list of default values. See the section “Description of the monitoring values” on page 343 for the meanings.

2. Only the data types are to be output in default output format.

```
/SHOW-FT-MONITOR-VALUES INFORMATION=*TYPE
openFT(STD)   Monitoring (formatted)
MonOn=2012-02-17 15:36:12 PartnerSel=OPENFT  RequestSel=ONLY-ASYNC,ONLY-LOCAL
2012-02-17 15:40:01

 Name      Value
 ----------------
 ThNetbTtl INT
 ThNetbSnd INT
 ThNetbRcv INT
 ThDiskTtl INT
 ThDiskSnd INT
 ThDiskRcv INT
 ThRqto    INT
 ThSuct    INT
 ThAbrt    INT
 ThIntr    INT
 ThUsrf    INT
 ThCofl    INT
 ThCobr    INT
 StRqas    INT(100)
 StRqaa    INT(100)
 StRqwt    INT(100)
 StRqhd    INT(100)
 StRqsp    INT(100)
 StRqlk    INT(100)
 StCLim    INT
 StCAct    PERCENT
 StRqLim   INT
 StRqAct   PERCENT
 StOftr    BOOL
 StFtmr    BOOL
 StFtpr    BOOL
```

Explanation

The types in the Value column have the following significance:

INT Integer number (corresponds to INT(1))

INT(100) Numeric value with a scaling value of 100 in the format n.mm, where n is an integer and mm are decimal places.

PERCENT Percentage

BOOL Boolean value, ON / OFF

3. The monitoring value "throughput in netbytes" (ThNetbTtl) is to be displayed. The display is to be updated every 60 seconds and repeated three times (polling).

```
/SHOW-FT-MONITOR-VALUES NAME=ThNetbTtl,POLLING=*PAR(INTERVAL=60,NUMBER=3)
```

```
openFT(STD)   Monitoring (formatted)
MonOn=2012-02-19 10:44:09 PartnerSel=OPENFT,FTP  RequestSel=ONLY-ASYNC,ONLY-LOCAL
2012-02-19 12:45:33
 Name      Value
 ----------------
 ThNetbTtl 780107

2012-02-19 12:46:33
 ThNetbTtl 993051

2012-02-19 12:47:33
 ThNetbTtl 1049832
```

The repetitions are separated by intermediate header containing the current polling time.

5.34 SHOW-FT-OPTIONS Display operating parameters

Note on usage

User group: FT user and FT administrator

Alias name: FTSHWOPT

Functional description

The command SHOW-FT-OPTIONS can be used at any time to obtain the information listed below on the operating parameters of your FT system:

- Information on whether or not openFT has been started
- Name of the BCAM host
- Instance identification
- Maximum values for operation (maximum number of file transfer requests in the request file, maximum lifetime of requests, maximum number of processes and transport connections, maximum size of a transport unit)
- Security settings (FTAC security level of the partner systems, extended sender verification)
- Logging settings (scope, intervals for automatic deletion)
- Trace settings
- Settings for traps (console traps, SNMP traps, ADM traps)
- Settings for the monitoring functions

Format

SHOW-FT-OPTIONS / **FTSHWOPT**
OUTPUT = ***SYSOUT**(...) / ***SYSLST**(...)
***SYSOUT**(...) / ***SYSLST**(...)
| **LAYOUT** = ***STD** / ***CSV** / ***BS2-PROC** / ***ZOS-PROC**

Operands

OUTPUT =
Output medium.

OUTPUT = *SYSOUT(...)
Output takes place on SYSOUT.

OUTPUT = *SYSLST(...)
Output takes place on SYSLST.

LAYOUT = *STD
Output is put into a user-friendly form for reading.

LAYOUT = *CSV
Output takes place in **C**haracter **S**eparated **V**alues format. This is a special tabular format, widely used in the PC world, where the individual fields are separated by semicolons “;“ (see section “Output in CSV format” on page 135).

LAYOUT = *BS2-PROC
The operating parameters are output as a command sequence. This can be called as an SDF procedure at BS2000/OSD systems in order to recreate the identical operating parameters.
If this output is redirected to a file using the SYSFILE command, you should note that the BS2000 SYSFILE management prefixes each line with the space (printer feed control character). The first column of the file must therefore be removed before the procedure generated in this way can be called.

LAYOUT = *ZOS-PROC
The operating parameters are output as a command sequence. This can be called as a Clist procedure at z/OS systems in order to recreate the identical operating parameters.

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
88	32	CMD0221	Error during OPS generation.
35	64	FTR1035	Command only permissible for FT administrator.
2	0	FTR2225	Information output canceled.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

The following table shows the OPS variables for the command SHOW-FT-OPTIONS.

Element	**Type**	**Output**
REQ-LIM	Integer	
TASK-LIM	String	
CONN-LIM	Integer	
TRANSPORT-UNIT-SIZE	Integer	
PARTNER-CHECK	String	*STD / *TRANSP-ADDR
SEC-LEV	String	Value / *BY-PARTNER-ATTRIBUTES
TRACE	Struct	
.STATE	String	*ON / *OFF
.OUT	String	*FILE / empty
.PARTNER-SEL	Struct	
.OPENFT	String	*YES / *NO
.FTAM	String	*YES / *NO
.FTP	String	*YES / *NO
.ADM	String	*YES / *NO
.REQUEST-SEL	Struct	
.SYNC	String	*YES / *NO
.ASYNC	String	*YES / *NO
.LOCAL	String	*YES / *NO
.REMOTE	String	*YES / *NO
.OPTIONS	Struct	
.BULK-DATA	String	*YES / *NO
LOG	Struct	
.TRANS-F	String	*ON / *OFF / *FAILURE
.FTAC	String	*ON / *REJECTED / *MODIFICATIONS
.ADM	String	*ON / *OFF / *FAILURE / *MODIFICATIONS
MAX-REQ-LIFETIME	String	*UNLIMITED / max-request-lifetime
SNMP-TRAPS	Struct	
.SUBSYSTEM-STATE	String	*OFF / *ON
.FT-STATE	String	*OFF / *ON
.PARTNER-STATE	String	*OFF / *ON
.PARTNER-UNREACHABLE	String	*OFF / *ON

Element	**Type**	**Output**
.REQUEST-QUEUE-STATE	String	*OFF / *ON
.TRANSFER-SUCCESS	String	*OFF / *ON
.TRANSFER-FAILURE	String	*OFF / *ON
CONSOLE-TRAPS[1]	String	*OFF / *ON
CONS-TRAPS	Struct	
.SUBSYSTEM-STATE	String	*OFF / *ON
.FT-STATE	String	*OFF / *ON
.PARTNER-STATE	String	*OFF / *ON
.PARTNER-UNREACHABLE	String	*OFF / *ON
.REQUEST-QUEUE-STATE	String	*OFF / *ON
.TRANSFER-SUCCESS	String	*OFF / *ON
.TRANSFER-FAILURE	String	*OFF / *ON
ADM-TRAPS	Struct	
.DESTINATION	Struct	
. PARTNER	String	Value
.SELECTION	Struct	
.FT-STATE	String	*OFF / *ON
.PARTNER-STATE	String	*OFF / *ON
.PARTNER-UNREACHABLE	String	*OFF / *ON
.REQUEST-QUEUE-STATE	String	*OFF / *ON
.TRANSFER-SUCCESS	String	*OFF / *ON
.TRANSFER-FAILURE	String	*OFF / *ON
ADM-CONN-LIM	Integer	Value
HOST-NAME	String	Name of the BCAM host
IDENTIFICATION	String	Identification of the local openFT instance
DYNAMIC-PARTNERS	String	*ON / *OFF
KEY-LEN	Integer	Value
STARTED	String	*YES / *NO
OPENFT-APPLICATION	String	*STD / Value
FTAM-APPLICATION	String	*STD / Value
FTP-PORT	String	*NONE / Value
OPENFT-STD	String	*STD / Value
ADM-PORT	String	Value

Element	**Type**	**Output**
OPENFT-APPL-STATE	String	*DISABLED / *ACTIVE / *INACTIVE
FTAM-APPL-STATE	String	*NAVAIL / *DISABLED / *ACTIVE / *INACTIVE
FTP-STATE	String	*NAVAIL / *DISABLED / *ACTIVE / *INACTIVE
ADM-STATE	String	*DISABLED / *ACTIVE / *INACTIVE
MONITORING	Struct	
.STATE	String	*ON / *OFF
.PARTNER-SEL	Struct	
.OPENFT	String	*YES / *NO
.FTAM	String	*YES / *NO
.FTP	String	*YES / *NO
.REQUEST-SEL	Struct	
.SYNC	String	*YES / *NO
.ASYNC	String	*YES / *NO
.LOCAL	String	*YES / *NO
.REMOTE	String	*YES / *NO
ACTIVE-APPLICATIONS	Struct	
.OPENFT	String	*ON / *OFF
.FTP	String	*ON / *OFF
.ADM	String	*ON / *OFF
ENC-MAND	Struct	
.IN	String	*YES / *NO
.OUT	String	*YES / *NO
DEL-LOG	Struct	
.STATE	String	*ON / *OFF
.RETENTION	Integer	Value
.REPEAT	String	*DAILY / *WEEKLY / *MONTHLY
.DAY	Integer	Value
.TIME	String	hh:mm:ss
ENC-MAND	Struct	
.IN	String	*YES / *NO
.OUT	String	*YES / *NO

[1] Now only support for reasons of compatibility. The value is only set if all the console traps are activated (*ON) or if all the console traps are deactivated (*OFF).

Meaning of the output of the OPS variables

Only the OPENTFT-STD variable is described below. The meanings of the other variables correspond to the associated output parameters of SHOW-FT-OPTIONS, see page 358.

OPENFT-STD
Port number used to address openFT partners if these are addressed via their host names without any port number specification.
*STD means that the default port number 1100 is used.
The value can be modified using the OPENFT-STF operand in the MODIFY-FT-OPTIONS command
Default setting following installation: *STD

5.34.1 Description of the output

Example

Default of the SHOW-FT-OPTIONS command, i.e. the operating parameters have not been modified since installation.

```
/SHOW-FT_OPTIONS
STARTED PROC-LIM CONN-LIM ADM-CLIM RQ-LIM MAX-RQ-LIFE TU-SIZE KEY-LEN
  YES       2       16         8     2000       30       65535   2048
PTN-CHK DYN-PART SEC-LEV  FTAC-LOG FT-LOG ADM-LOG     ENC-MAND
  STD       ON   B-P-ATTR    ALL    ALL    ALL           NO
OPENFT-APPL      FTAM-APPL         FTP-PORT           ADM-PORT
*STD             *STD              21                 11000
ACTIVE           ACTIVE            ACTIVE             ACTIVE
HOST-NAME         IDENTIFICATION
*NONE             BS2FTPC

DEL-LOG  ON  AT     RETPD   ADM-TRAP-SERVER
 OFF   DAILY 00:00    14    *NONE

TRAP: SS-STATE FT-STATE PART-STATE PART-UNREA RQ-STATE TRANS-SUCC TRANS-FAIL
CONS    OFF      OFF      OFF        OFF        OFF       OFF        OFF
SNMP    OFF      OFF      OFF        OFF        OFF       OFF        OFF
ADM              OFF      OFF        OFF        OFF       OFF        OFF

FUNCT:  SWITCH PARTNER-SELECTION    REQUEST-SELECTION    OPTIONS
MONITOR   OFF  ALL                  ALL
TRACE     OFF  ALL                  ALL                  NONE
```

Meaning of the output fields

STARTED
Specifies whether openFT is activated (via START-FT or automatically) or not.

PROC-LIM
Maximum number of tasks that can be reserved simultaneously for the execution of FT requests. The value is defined by the PROCESS-LIMIT operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: 2

CONN-LIM
Maximum number of transport connections that can be reserved for asynchronous file transfer requests. Since each transport connection can only process one request at a time, CONN-LIMIT also defines the maximum number of requests that can be processed simultaneously. One third of the transport connections are reserved for requests from remote systems. The value of CONN-LIMIT is defined by the CONNECTION-LIMIT operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: 8

ADM-CLIM
Maximum number of asynchronous administration requests including ADM traps that can be processed simultaneously. The value of ADM-CLIM is specified with the operand ADM-CONNECTION-LIM in the command MODIFY-FT-OPTIONS.
Default setting following installation: 8

RQ-LIM
Maximum number of FT requests that can be entered at the same time in the request queue of the local system. The value can be modified using the REQUEST-LIMIT operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: 2000

MAX-RQ-LIFE
Maximum number of days that an FT request is stored in the request file after its start time. When this period expires, the FT request is automatically removed from the request file. The value is defined in the MAX-REQUEST-LIFETIME operand of the MODIFY-FT-OPTIONS command.
Default setting following installation: 30

TU-SIZE
Maximum size of a transport unit in bytes. The value is defined with the TRANSPORT-UNIT-SIZE operand in the MODIFY-FT-OPTIONS command. The load placed on the transport system by openFT can be controlled using this operand.
Default setting following installation: 65535

KEY-LEN
Current length of the RSA key. 0 means that encryption is deactivated. The value is defined with the KEY-LENGTH operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: 2048

PTN-CHK
Defines whether or not enhanced sender checking is activated. The value is defined with the PARTNER-CHECK operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: STD

DYN-PART
specifies whether dynamic partners are permitted (*ON) or not (*OFF). The value is defined with the DYNAMIC-PARTNERS operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: ON

SEC-LEV
Local default value for the security level of the partner systems. This operand is only effective if FTAC functionality is being used. An important part of the access protection functions provided by this product lies in the allocation of security levels to remote systems. To this end, each system is allocated a security level designated using an integer in the range 1 to 100.

A default value for all remote systems is set using the SECURITY-LEVEL operand in the MODIFY-FT-OPTIONS command. All partners in the partner list for which the value STD is specified in the output of the SHOW-FT-PARTNERS command for SECLEV refer to this value.
This value is irrelevant for free dynamic partners (i.e. partner not entered in the partner list).
Default setting following installation: B-P-ATTR

FTAC-LOG
Scope for FTAC logging (ALL, MODIFY, REJECTED).
The scope of FTAC logging is specified in the LOGGING operand of the MODIFY-FT-OPTIONS command.
Default setting following installation: ALL

FT-LOG
Scope for FT logging (ALL, FAIL, NONE).
The scope of FT logging is specified in the LOGGING operand of the MODIFY-FT-OPTIONS command.
Default setting following installation: ALL

ADM-LOG
Scope of ADM logging (ALL, FAIL, MODIFY, NONE).
The scope of ADM logging is specified in the LOGGING operand of the MODIFY-FT-OPTIONS command.
Default setting following installation: ALL

ENC-MAND
Specifies whether user data encryption is mandatory for openFT requests.
The value can be modified with the ENCRYPTION-MANDATORY operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: NO

OPENFT-APPL
Port number used by the local openFT. *STD means that the default port number 1100 is used. The value is specified with the OPENFT-APPLICATION operand in the command MODIFY-FT-OPTIONS.
The second line specifies whether the asynchronous inbound server is activated for openFT (ACTIVE), deactivated (DISABLED) or unavailable (INACT). The ACTIVE-APPLICATIONS operand in the command MODIFY-FT-OPTIONS is used for activation and deactivation.
Default setting following installation: *STD

FTAM-APPL
Port number of the local FTAM server, where necessary supplemented by the transport selector, session selector and presentation selector. *STD means that the default value is used (port number 4800 and $FTAM as the transport selector).
The value can be modified with the FTAM-APPLICATION operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: *STD

FTP-PORT
Port number used by the local FTP server. The value is specified with the FTP-PORT operand in the command MODIFY-FT-OPTIONS.
The second line specifies whether the asynchronous inbound server is activated for FTP (ACTIVE/DISABLED) or is unavailable or not installed (INACT/NAVAIL). The ACTIVE-APPLICATIONS operand in the command MODIFY-FT-OPTIONS is used for activation and deactivation.
Default setting following installation: 21

ADM-PORT
Specifies the port number used by the local FT for remote administration. The default value is 11000. The value is specified with the ADM-PORT operand in the command MODIFY-FT-OPTIONS.
The second line specifies whether the asynchronous inbound server is activated for remote administration requests (ACTIVE), deactivated (DISABLED) or unavailable (INACT). The ACTIVE-APPLICATIONS operand in the command MODIFY-FT-OPTIONS is used for activation and deactivation.
Default setting following installation: 11000

HOST-NAME
Name of the BCAM host. The default value is *NONE, i.e. the real BCAM host is used. The value can be modified with the HOST-NAME operand in the MODIFY-FT-OPTIONSFT-MODOPT command.
Default setting following installation: *NONE

IDENTIFICATION
Instance identifier of the openFT instance currently set and the name of the local system. The instance identifier is defined with the IDENTIFICATION operand of the MODIFY-FT-OPTIONS command and is used to identify the instance in the partner systems.
Default setting following installation: Name of the local BCAM host

DEL-LOG
Specifies whether automatic deletion of log records is activated.
The values can be modified using the DELETE-LOGGING operand in the MODIFY-FT-OPTIONS command.
Default setting following installation: OFF

- ON: Day on which the records are to be deleted. A weekday (MON, TUE, WED, THU, FRI, SAT, SUN), a day of the month (1 through 31) or DAILY for daily deletion must be entered here.
  Default setting following installation: DAILY
- AT: Time (*hh:mm*) at which the records are to be deleted.
  Default setting following installation: 00:00
- RETPD: Minimum age of the records which are to be deleted (in days).
  Default setting following installation: 14

ADM-TRAP-SERVER
Name or address of the partner to which the ADM traps are sent.
*NONE means that the sending of ADM traps is deactivated.
The value is specified with the ADM-TRAPS=(DESTINATION=...) operand in the command MODIFY-FT-OPTIONS.
Default setting following installation: *NONE

TRAP
This section with the rows CONS, SNMP and ADM specifies the trap settings. The columns identify the events for which traps may be generated.

- SS-STATE: Subsystem state change (not for ADM traps)
- FT-STATE: State change of the openFT control process
- PART-STATE: Partner system state change
- PART-UNREA: Partner not reachable
- RQ-STATE: Request management state change
- TRANS-SUCC: Successfully completed requests
- TRANS-FAIL: Failed requests

  The possible values are ON or OFF.
  Default setting following installation: OFF (for all columns)

The following rows specify the settings for the various trap types:

CONS
Settings for console traps FTR03XXX. This is specified with the CONSOLE-TRAPS operand in the command MODIFY-FT-OPTIONS.

SNMP
Setting for SNMP traps. This is specified with the SNMP-TRAPS operand in the command MODIFY-FT-OPTIONS.

ADM
Setting for ADM traps to be output to the ADM trap server. This is specified with the ADM-TRAPS=(SELECTION=...) operand in the command MODIFY-FT-OPTIONS.

FUNCT
This section specifies the settings for monitoring (MONITOR) and tracing (TRACE).
The values can be modified with the TRACE operand in the MODIFY-FT-OPTIONS command.
The columns have the following meanings:

- SWITCH: Function activated (ON) or deactivated OFF
  Default setting following installation: OFF
- PARTNER-SELECTION: Selection according to protocol type of the partner system: ALL, OPENFT, FTP, ADM (only with TRACE), NONE
  Default setting following installation: ALL
- REQUEST-SELECTION: Selection according to request type: ALL, ONLY-ASYNC, ONLY-SYNC, ONLY-LOCAL, ONLY-REMOTE
  Default setting following installation: ALL
- OPTIONS (only with TRACE): NONE, NO-BULK-DATA (= minimal trace, i.e. no bulk data)
  Default setting following installation: NONE

The following rows specify what the settings apply to:

MONITOR
Setting for monitoring. This is specified with the MONITORING operand in the command MODIFY-FT-OPTIONS.
Default setting following installation: OFF

TRACE
Setting for trace function. This is specified with the TRACE operand in the command MODIFY-FT-OPTIONS.
Default setting following installation: NONE

5.35 SHOW-FT-PARTNERS Display partner systems

Note on usage

User group: FT user and FT administrator

Alias name: FTSHWPTN

Functional description

The SHOW-FT-PARTNERS command is used to obtain the following information on partner systems included in the partner list :

– the names of the remote systems in the partner list,

– the status of the requests with the remote systems (activated or deactivated),

– priority assigned to the partner system,

– the setting for the openFT trace function on the partner system,

– the security level assigned to the remote system. Tthis security level applies only if FTAC functionality is used. The information can then also be obtained using the SHOW-FT-RANGE command.

– the number of not yet completed file transfer requests submitted in the local system,

– the number of file transfer requests submitted in the remote systems for the local system,

– the partner address.

– the type of sender checking,

– in the case of output in CSV format or to an OPS variable: also the time of the last access and the authentication level.

i SHOW-FT-PARTNERS with the PARTNER=*ALL operand (default value) displays all **entered** dynamic partners. These can be recognized from the fact that they have no name. If you only want to output detailed information on one entered dynamic partner, you must specify the partner's address in the PARTNER operand.
In the case of the SHOW-FT-PARTNERS command openFT does not check whether an address is valid. If, for example, you specify a random address of a free dynamic partner, this will be displayed with the default properties of a free dynamic partner.

Format

```
SHOW-FT-PARTNERS / FTSHWPTN

 PARTNER = *ALL / <text 1..200 with-low>
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
    *SYSOUT(...) / *SYSLST(...)
     |  LAYOUT = *STD / *CSV / *BS2-PROC / *ZOS-PROC
,STATE = *ALL / *ACTIVE / *DEACT / *INSTALLATION-ERROR / *NO-CONNECTION / *NOT-ACTIVE /
             *AUTOMATIC-DEACTIVATION / *INACTIVE-BY-AUTOMATIC-DEACT
,INFORMATION = *STD / *ALL
```

Operands

PARTNER =
Partner system or systems about which information is to be output.

PARTNER = *ALL
Information on all partner systems is output.

PARTNER = <text 1..200 with-low>
Name or address of the partner system or group of partner systems about which information is to be output.
If you enter a name then you have two options:
You can either enter a unique partner name (1 - 8 alphanumeric characters) or a group of partners identified by a 1 to 7-character specification followed by an asterisk (*).
For more information on partner addresses, see section “Defining partner properties” on page 44

OUTPUT =
Output medium.

OUTPUT = *SYSOUT(...)
Output is sent to SYSOUT.

OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = *STD
Output is formatted using a standard layout that can be easily read by the user.

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon “;“ (see page 135).

LAYOUT = *BS2-PROC
Output is supplied in the form of MODIFY-FT-PARTNER commands, which precisely define the partners involved. This enables the partner entries to be saved for a later reconstruction, to use them for an openFT operation on BS2000.
If this output is redirected to a file by using the SYSFILE command, it should be noted that the BS2000 Sysfile Management inserts a blank (i.e., a linefeed character) before each line. The first column of the file must hence be stripped before the procedure generated by this method can be called. We therefore recommend that you use the START-OPENFTPART command, which performs this task for the user.

LAYOUT = *ZOS-PROC
Output is supplied in the form of FTMODPTN commands, which precisely define the partners involved. This enables the partner entries to be saved for a later reconstruction, to use them for an openFT operation on z/OS (.

STATE =
The scope of the output can be limited by the optional selection criteria in STATE. For an explanation of the selection criteria see page 369.

STATE = _*ALL_
The output is not limited by selection criteria.

STATE = *ACTIVE
All partner systems in the ACTIVE state are displayed.

STATE = *DEACT
All partner systems in the DEACT state are displayed.

STATE = *INSTALLATION-ERROR
All partner systems in the LUNK, RUNK, LAUTH, RAUTH, NOKEY and IDREJ state are displayed.

STATE = *NO-CONNECTION
All partner systems in the NOCON and DIERR state are displayed.

STATE = *NOT-ACTIVE
All partner systems not in the ACTIVE state are displayed.

STATE = *AUTOMATIC-DEACTIVATION
All partner systems are output which were assigned AUTOMATIC-DEACTIVATION.

STATE = *INACTIVE-BY-AUTOMATIC-DEACT
All partner systems are output which were actually deactivated using the option AUTOMATIC-DEACTIVATION.

INFORMATION = _*STD_ / *ALL
Use this operand to control the scope of the information output. On *ALL, expanded address information is output, in addition to the standard information.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	No partner available for the selection criteria.
83	32	CMD0221	Internal error.
88	32	CMD0221	Error during OPS generation.
35	64	FTR1035	The user is not authorized to use this command.
45	64	FTR1045	No partner found in partner list.
2	0	FTR2225	Information output cancelled.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

The following table shows the OPS variables for the command SHOW-FT-PARTNERS.

Element	Type	Output
PARTNER-NAME	String	
STA	String	*ACTIVE / *INACTIVE / *NO-CONN / *LOC-UNKNOWN /*REM-UNKNOWN / *ACTIVE (AUTO-DEACTIVATE) / *INACTIVE (BY- AUTOMATIC-DEACTIVATION) / *LOC-AUTH-FAIL / *REM-AUTH-FAIL / *DATA-INTEGRITY-ERROR / *NO-KEY / *ID-REJ
SEC-LEV	Integer/ String	VALUE / *B-P-ADDR
TRACE [1]	String	*ON / *OFF / *BY-FT-OPT
LOC	Integer	Value
REM	Integer	Value
PARTNER-ADDR	String	Value
PRIO	String	*NORM / *HIGH / *LOW
AUTHENTICATION-LEVEL	Integer	1 / 2 / empty
LAST-ACCESS-DATE	String	Value / empty
ADDR-TYPE [2]	String	*OPENFT / *PRESENTATION / *TCP-IP
OPENFT-ADDR [3]	Struct	
.PROCESSOR	String	Value
.ENTITY	String	Value
.NETWORK-ADDR	String	Value
.TRANS-SEL	String	Value
.PORT	String	port number

Element	Type	Output
.PARTNER-CHECK	String	*FTOPT / *STD / *TRANSP-ADDR / *AUTH
.AUTH-MAND	String	*YES / *NO
.IDENTIFICATION	String	Value
.SESSION-ROUTING	String	*ID or empty
PRESENTATION-ADDR [4]	Struct	
.NETWORK-ADDR	String	Value
.TRANSPORT-SEL	String	Value
.SESSION-SEL	String	Value
.PRESENTATION-SEL	String	Value
.PORT	String	Value
TCP-IP-ADDR [5]	Struct	
.PORT	String	Value
ADM-ADDR [6]	Struct	
.PROCESSOR	String	Value
.ENTITY	String	Value
.NETWORK-ADDR	String	Value
.TRANS-SEL	String	Value
.PORT	String	Port number
.PARTNER-CHECK	String	*FTOPT / *STD / *TRANSP-ADDR /*AUTH
.AUTH-MAND	String	*YES / *NO
.IDENTIFICATION	String	Value
.SESSION-ROUTING	String	*ID / empty
INBOUND-STATE	String	*ACTIVE / *INACTIVE
REQ-PROC	String	*STD / *SERIAL

[1] TRACE is only displayed for openFT partners.

[2] Only the address structure corresponding to the ADDR-TYPE element is displayed.

[3] Only applies to openFT partners.

[4] Only applies to FTAM partners.

[5] Only applies to FTP partners.

[6] Only applies to ADM partners

Example

Request information on all remote systems entered in the partner list:

Short output:

```
/SHOW-FT-PARTNERS INF=*STD
NAME     STATE SECLEV   PRI  TRACE   LOC    REM P-CHK ADDRESS
         ACT    90      NORM FTOPT     0      0 FTOPT TEST011N
HOSTABS2 ACT   B-P-ATTR NORM FTOPT     0      0 FTOPT HOSTABS2
HOSTBBS2 ACT   STD      NORM FTOPT     0      0 FTOPT HOSTBBS2
FOREIGN  ACT    10      NORM FTOPT     0      0       ftam://PC3:102.ftam.
                                                      ftam.ftam
FTAMPC   ACT    30      NORM FTOPT     0      0       ftam://PC2:.$ftam
FTAMUX   ACT    30      NORM FTOPT     0      0       ftam://UNIX3
PCUSER   ACT    40      LOW  FTOPT     0      0 FTOPT %IP123.23.99.120
PC1      ACT    40      LOW  FTOPT     0      0 FTOPT PC1
UNIX1    ACT    50      HIGH FTOPT     0      0 FTOPT UNIX1
UNIX2    ACT    50      HIGH FTOPT     0      0 FTOPT UNIX2:102
FTPUX1   ACT   STD      NORM FTOPT     0      0       ftp://%IP132.19.122.50
```

Long output:

```
/SHOW-FT-PARTNERS INF=*ALL

NAME     STATE SECLEV   PRI  TRACE  LOC  REM P-CHK ADDRESS
         INBND REQU-P                                ROUTING  IDENTIFICATION
         ACT   90       NORM FTOPT    0    0 FTOPT TEST011N
         ACT   STD                                            TEST011N
HUGO     ACT   STD      NORM FTOPT    0    0 FTOPT HUGO
         ACT   STD                                            %.HUGO.$FJAM
HOSTABS2 ACT   B-P-ATTR NORM FTOPT    0    0 FTOPT HOSTABS2
         ACT   STD                                            HOSTABS2.FUJI.NET
HOSTBBS2 ACT   STD      NORM FTOPT    0    0 FTOPT HOSTBBS2
         ACT   STD                                            HOSTBBS2.CLOUD.NET
FOREIGN  ACT    10      LOW  FTOPT    0    0       ftam://PC3:102.ftam.
         ACT   STD                                            ftam.ftam
FTAMPC   ACT    30      NORM FTOPT    0    0       ftam://PC2:.$ftam
         ACT   STD                                            ftamw.ftam2
FTAMUX   ACT    30      NORM FTOPT    0    0       ftam://UNIX3
         ACT   STD                                            ftamx.ftam3
PCUSER   ACT    40      LOW  FTOPT    0    0 FTOPT %IP123.23.99.120
         ACT   STD                                            %IP123.23.99.120
PC1      ACT    40      LOW  FTOPT    0    0 FTOPT PC1
         ACT   STD                                            PC1.FUSI.NET
UNIX1    ACT    50      HIGH FTOPT    0    0 FTOPT UNIX1
         ACT   STD                                            UNIX1.DREAM.NET
UNIX2    ACT    50      HIGH FTOPT    0    0 FTOPT UNIX2:102
         ACT   STD                                            %.UNIX2.$FJAM
FTPUX1   ACT   STD      NORM FTOPT    0    0       ftp://%IP132.19.122.50
         ACT   STD
```

The information displayed is explained below:

NAME
Symbolic names of the remote systems entered in the partner list.
This field remains empty for dynamic partners (see the first line in the example).

STATE
Status of the partner system.

ACT
The partner system is active.

DEACT
The partner system is deactivated.

NOCON
The transport connection setup failed.

LUNK
The local system is unknown on the remote FT system.

RUNK
The partner system is unknown on the local transport system.

ADEAC
The partner system is active. It is deactivated if the connection cannot be established. This state is only displayed if STATE=*AUTOMATIC-DEACTIVATION has been specified; otherwise, these partner systems are maintained under the ACT status.

AINAC
The partner system was deactivated following several unsuccessful attempts to establish a connection. This status is only possible if STATE=*AUTOMATIC-DEACTIVATION has been specified.

LAUTH
The local system could not be authenticated in the partner system. A current, public key of the local openFT instance must be made available to the partner system.

RAUTH
The partner system could not be authenticated in the local system. A current, public key of the partner system must be imported to the SYSKEY library.

DIERR
A data integrity error was detected on the connection to the partner system. This can be due either to an error in the transport system, or to manipulation attempts along the transfer route. The connection was terminated but the affected request was not (if it is restartable).

NOKEY
The partner does not accept a connection without encryption, but no key is present in the local system. A new key must be created using CREATE-FT-KEY-SET .

IDREJ
The partner or a go-between instance does not accept the instance ID sent from the local system. You must check to see if the local instance ID is consistent with the entry in the partner's partner list.

SECLEV
Security level assigned to the remote system when it was entered in the partner list. These security levels apply only if the FTAC-BS2000 is also implemented. STD stands for the default security level set with the MODIFY-FT-OPTIONS command.

PRI
Priority of a partner with respect to the processing of requests. The possible values are NORM, LOW and HIGH.

TRACE
Trace setting. You may specify the values ON, OFF and FTOPT (if MODIFY-FT-PARTNER is specified, TRACE=*BY-FT-OPTIONS).

LOC
Number of FT requests that have been submitted in the local system and that address the FT system specified with PARTNER.

REM
Number of FT requests that have been submitted in the remote FT system and addressed to the local FT system. The remote system is specified in PARTNER.

P-CHK
Type of sender checking for the current partner:

FTOPT
The global setting is valid.

T-A
The expanded sender checking is enabled for specific partners.

STD
The expanded sender checking is disabled for specific partners.

AUTH
With the aid of its public key in the SYSKEY library, the partner is subjected to an identity check ("authenticated") by cryptographic means. The partner support the authentication level 2.

AUTH!
With the aid of its public key in the SYSKEY library, the partner is subjected to an identity check ("authenticated") by cryptographic means. The partner support the authentication level 1.

NOKEY
No valid key is available from the partner system although authentication is required.

AUTHM
Authentication must be used.

ADDRESS
Partner address under which the remote system can be accessed. For more information on partner addresses, see section “Defining partner properties” on page 44.

IDENTIFICATION
Instance ID of the partner (also see the ADD-FT-PARTNER command on page 136).

ROUTING
SESSION-ROUTING-INFO of the partner, where required (also see the ADD-FT-PARTNER command, on page 136).

INBND
State of the partner for inbound requests:

ACT
Inbound function is activated, i.e. requests issued remotely are processed.

DEACT
Inbound function is deactivated, i.e. requests issued remotely are rejected.

REQU-P
Operating mode for asynchronous outbound requests:

STD
Requests to this partner can be processed in parallel.

SERIAL
Requests to this partner are always processed serially.

5.36 SHOW-FT-PROFILE Display admission profile

Note on usage

User group: FTAC user and FTAC administrator

Prerequisite for using this command is the use of openFT-AC.

Functional description

With the command SHOW-FT-PROFILE, FTAC users can obtain information about their admission profiles. The FTAC administrator can obtain information about all the admission profiles in his/her system.

Either the contents of the selected admission profile or only its name can be output. It is not possible to use SHOW-FT-PROFILE to access defined passwords or transfer admissions defined in the profile! If a transfer admission is forgotten, a new one must be specified using MODIFY-FT-PROFILE.

Format

```
SHOW-FT-PROFILE

 NAME = *ALL / <alphanum-name 1..8> / *STD
,SELECT-PARAMETER = *OWN / *PARAMETERS(...)
    *PARAMETERS(...)
      |  TRANSFER-ADMISSION = *ALL / *NOT-SPECIFIED / <alphanum-name 8..32> /
      |                                  <c-string 8..32 with-low> / <x-string 15..64> / *SECRET
      | ,OWNER-IDENTIFICATION = *OWN / *ALL / <name 1..8>
,INFORMATION = *ONLY-NAMES / *ALL
,OUTPUT = *SYSOUT(...) / *SYSLST(...)
    *SYSOUT(...) / *SYSLST(...)
      |  LAYOUT = *STD / *CSV
```

Operands

NAME =
Name of the admission profile you wish to view.

NAME = *ALL
Views all admission profiles.

NAME = <alphanum-name 1..8>
Views the admission profile with the specified name.

NAME = *STD
Displays the default admission profile for your own user ID.

SELECT-PARAMETER =
Selection criteria for the admission profiles you wish to view.

SELECT-PARAMETER = *OWN
Views all the admission profiles of which you are the owner. This means that you can view all the admission profiles which are assigned to your user ID.

SELECT-PARAMETER = *PARAMETERS(...)
Selection criteria with which you can access your admission profiles.

TRANSFER-ADMISSION =
Transfer admission defined in an admission profile as a selection criterion. Only the FTAC administrator can enter the user IDs of other users.

TRANSFER-ADMISSION = *ALL
TRANSFER-ADMISSION is not used as a selection criterion.

TRANSFER-ADMISSION = *NOT-SPECIFIED
Only admission profiles for which no transfer admission has been specified are displayed.

TRANSFER-ADMISSION = <alphanum-name 8..32> / <c-string 8..32 with-low> / <x-string 15..64>
Views the admission profile which can be addressed with this transfer admission.

TRANSFER-ADMISSION = *SECRET
The system prompts you to enter the transfer admission. However, this does not appear on the screen.

OWNER-IDENTIFICATION =
Specifies, whose admission profiles you wish to view.

OWNER-IDENTIFICATION = *OWN
Views only your own admission profile.

OWNER-IDENTIFICATION = *ALL
The FTAC administrator can view all admission profiles, regardless of who the owner is.

OWNER-IDENTIFICATION = <name 1..8>
The FTAC user can only access his/her own admission profiles; the output corresponds to *OWN. The FTAC administrator can view the admission profiles of any FTAC user with this parameter.

INFORMATION =
Scope of information desired.

INFORMATION = <u>*ONLY-NAMES</u>
FTAC only outputs the name of the admission profile and indicates whether it is privileged or blocked. An “*“ is output for privileged profiles and a “!“ for blocked profiles.

INFORMATION = *ALL
FTAC outputs the contents of the admission profile, excluding any passwords and the transfer admission.

OUTPUT =
Output medium for the information.

OUTPUT = <u>*SYSOUT</u>(...)
Output is sent to SYSOUT.

OUTPUT = *SYSLST(...)
Output is sent to SYSLST.

LAYOUT = <u>*STD</u>
Output is formatted using a standard layout that can be easily read by the user.

LAYOUT = *CSV
Output is supplied in CSV (**C**haracter **S**eparated **V**alues) format. This is a widely used tabular format, especially in the PC environment, in which individual fields are separated by a delimiter, which is usually a semicolon “;“ (see section “Output in CSV format” on page 135).

Command return codes

(SC2)	SC1	Maincode	Meaning
0	64	FTC0052	The information output was interrupted.
0	64	FTC0053	No FT profile exists which meets the specified criteria.
0	0	FTC0054	No information exists for the specified criteria.
0	64	FTC0153	The owner identification entered is not the user’s own ID.
0	64	FTC0171	The profile entered does not exist.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133.

OPS variables

The following table shows the OPS variables of the SHOW-FT-PROFILE command with the operand INF=*ALL. The underlined values apply to the output with INF=*ONLY-NAMES.

Element	Type	Output
PROF-NAME	String	
PRIV	String	*YES / *NO
TRANS-ADM	String	*NSPEC / *SECRET
DUPLICATED	String	*YES / *NO
LOCKED-BY	Struct	
.IMPORT	String	*YES / *NO
.ADM	String	*YES / *NO
.USER	String	*YES / *NO
EXPIRED	String	*YES / *NO
USER-ADM	Struct	
.USER-ID	String	User-ID
.ACC	String	Account number / *FIRST / *NSPEC / *NONE / *NRES
.PASSWORD	String	*OWN / *NSPEC / *NONE / *YES
EXP-DATE	String	yyyy-mm-dd / *NRES
USAGE	String	*PUBLIC / *PRIVATE / *NSPEC
IGNORE	Struct	
.OBS	String	*YES / *NO
.OBR	String	*YES / *NO
.IBS	String	*YES / *NO

Element	**Type**	**Output**
.IBR	String	*YES / *NO
.IBP	String	*YES / *NO
.IBF	String	*YES / *NO
INITIATOR	String	*LOC / *REM / *NRES
TRANS-DIR	String	*FROM / *TO / *NRES
MAX-PART-LEV	String	Maximum security level / *NRES
PARTNERS	Array (1-50)	One or several partners / *NRES
FILE-NAME	String	File name / *NRES
LIBRARY	String	*YES / *NO / *NRES / Library
FILE-NAME-PREFIX	String	*YES / *NO
ELEM	Struct	
.NAME	String	Name / *NRES / *NONE
.PREFIX	String	*YES / *NO
.VERSION	String	Version / *STD / *NONE / *NRES
.TYPE	String	Type / *NRES / *NONE
FILE-PASSWORD	String	*YES / *NRES / *NONE
WRITE	String	*NEW / *EXT / *REPL / *NRES
PROC-ADM	Struct	
.USER-ID	String	User-ID / *NRES / *SAME
.ACC	String	Account number / *NRES / *SAME / *NONE
.PASSWORD	String	*NONE / *YES / *NRES / *SAME
SUCC	Struct	
.PROC	String	Commands / *NONE / *NRES / *EXPANSION
.PREFIX	String	Prefix / *NONE
.SUFFIX	String	Suffix / *NONE
FAIL	Struct	
.PROC	String	Commands / *NONE / *NRES / *EXPANSION
.PREFIX	String	Prefix / *NONE
.SUFFIX	String	Suffix / *NONE
TRANS-FILE	String	*ALLOWED / *NOT-ALLOWED
MOD-FILE-ATTR	String	*ALLOWED / *NOT-ALLOWED
READ-DIR	String	*ALLOWED / *NOT-ALLOWED
FILE-PRO^C	String	*ALLOWED / *NOT-ALLOWED

Element	Type	Output
ACC-ADM	String	*ALLOWED / *NOT-ALLOWED
REM-ADM	String	*ALLOWED / *NOT-ALLOWED
ADM-TRAP-LOG	String	*ALLOWED / *NOT-ALLOWED
TEXT	String	Text / *NONE
DATA-ENC	String	*YES / *NO / *NRES
LAST-MOD	Struct	
.DATE	String	yyyy-mm-dd / *NONE
.TIME	String	hh:mm:ss / *NONE

Example 1

The FTAC administrator wishes to view the admission profile UMSAWARE with the command SHOW-FT-PROFILE to determine if the profile might endanger data protection:

```
/SHOW-FT-PROFILE␣NAME=UMSAWARE, -
/     SELECT-PARAMETER=(OWNER-IDENTIFICATION=STEVEN),INFORMATION=*ALL
```

Short form:

```
/SHOW-FT-PROF␣UMSAWARE,(,STEVEN),*ALL
```

The output takes the following form:

```
%UMSAWARE
% EXP-DATE    = 20121231
% IGN-MAX-LEV = (IBR)
% FILE        = UMSATZ
% USER-ADM    = (STEFAN,M4711,OWN)
% PROC-ADM    = SAME
% SUCC-PROC   = NONE
% FAIL-PROC   = NONE
% FT-FUNCTION = (TRANSFER-FILE, MODIFY-FILE-ATTRIBUTES,
%               READ-FILE-DIRECTORY, FILE-PROCESSING)
% DATA-ENC    = YES
% LAST-MODIF  = 2012-07-11 13:38:11
```

The first line shows the name of the admission profile. EXP-DATE shows the expiration date of the admission profile. The next two lines show the settings which Steven made in the command CREATE-FT-PROFILE using the parameter IGNORE-MAX-LEVELS=(INBOUND-RECEIVE=*YES) and FILE-NAME= PROFIT. The values for USER-ADMISSION and PROCESSING-ADMISSION have not been set by Steven, but rather the default values have been used. The output SUCC-PROC=*NONE and FAIL-PROC=*NONE means that no follow-up processing is permitted. The output DATA-

ENC=YES shows that Steven is especially careful, because this means that requests are only accepted if the user data is encrypted. Steven set this by using DATA-ENCRYPTION=*YES in the CREATE-FT-PROFILE command. The timestamp of the most recent change is shown under LAST-MODIF.

The timestamp is also updated if you do not change the properties of the profile, i.e. if you enter MODIFY-FT-PROFILE only with the parameter NAME, but no other parameters.

ℹ Please note that as a rule not all properties of a profile are displayed. For example, optional parameters which do not differ from the default are not shown.

Example 2

The FTAC administrator examines the admission profile TESTPROF using the SHOW-FT-PROFILE command to determine whether file processing is possible with this profile. The command is as follows:

```
/SHOW-FT-PROFILE˽NAME=TESTPROF, -
/     SELECT-PARAMETER=(OWNER-IDENTIFICATION=STEVEN),INFORMATION=*ALL
```

Short form:

```
/SHOW-FT-PROF˽TESTPROF,(,STEVEN),INF=*ALL
```

The output has the following form:

```
%TESTPROF
% INITIATOR   = REMOTE
% USER-ADM    = (STEVEN,*FIRST,OWN)
% PROC-ADM    = SAME
% FT-FUNCTION = (TRANSFER-FILE,FILE-PROCESSING)
% LAST-MODIF  = 2012-01-31 15:03:44
```

The first line of the output displays the name of the admission profile. The second line indicates that the profile can only be used for requests initiated in the remote system. Steven has specified the value *FIRST for ACCOUNT in USER-ADMISSION; this means that the first account number assigned to the home pubset of the specified user ID in the system is used for account assignment in the case of transfer requests. As a result, it is unaffected by any changes to the account number. However, Steven has not specified a value for PROCESSING-ADMISSION and the default value SAME is therefore used. This means that the values are taken over from USER-ADMISSION. The FT-FUNCATION line indicates that the examined profile supports both pre-processing and file transfer requests. The last row specifies when the profile was last modified. The timestamp is also updated if you do not change the properties of the profile, i.e. if you enter MODIFY-FT-PROFILE only with the parameter NAME, but no other parameters.

Example 3

The FT administrator wishes to view the profile REMADMIN that has been set up for remote administration by a remote administrator.

```
/SHOW-FT-PROFILE␣NAME=REMADMIN,INFORMATION=*ALL
```

Output has the following form:

```
%REMADMIN
% USER-ADM    = (BS2ADMIN,,YES)
% FT-FUNCTION = (REMOTE-ADMINISTRATION)
% LAST-MODIF  = 2012-02-21 15:31:29
```

The output REMOTE-ADMINISTRATION for FT-FUNCTION indicates that the profile is permitted to perform remote administration. This means that the profile can be used by remote administrators to administer the local openFT instance. These remote administrators must also be configured in the remote administration server.

5.37 SHOW-FT-RANGE Display partner systems

Note on usage

User group: FTAC user and FTAC administrator

Prerequisite for using this command is the use of openFT-AC.

Functional description

The command SHOW-FT-RANGE is used to list the partner systems with which you can communicate by file transfer. In addition to indicating the name of the partner system, the security level is output which the FT administrator assigned to this system in the partner list. To determine which basic functions you are permitted to use, you must use the command SHOW-FT-ADMISSION-SET to obtain information on your admission set (see page 306).

The FTAC administrator can use SHOW-FT-RANGE to list all partner systems with which his/her FT system can communicate using file transfer. Furthermore, he/she can find out for any user in his/her system which partner systems can be accessed by this user.

Format

```
SHOW-FT-RANGE

 USER-IDENTIFICATION = *OWN / <name 1..8>

,SELECT-PARAMETER = *ALL / *PARAMETERS(...)

    *PARAMETERS(...)
      |   PARTNER = *ALL / <text 1..200 with-low>

,OUTPUT = *SYSOUT(...) / *SYSLST(...)

    *SYSOUT(...) / *SYSLST(...)
      |   LAYOUT = *STD / *CSV
```

Operands

USER-IDENTIFICATION =
User ID for which you would like to have a list of accessible partner systems.

USER-IDENTIFICATION = *OWN
The FTAC user receives all the partner systems with which he/she can use at least one basic function.
The FTAC administrator receives all accessible partner systems.

USER-IDENTIFICATION = <name 1..8>
The FTAC user can only enter his/her own user ID here, the output corresponds to *OWN.
The FTAC administrator can enter any user ID for which he/she would like to view the accessible partner systems.

SELECT-PARAMETER =
Specifies selection criteria for the partner systems.

SELECT-PARAMETER = *ALL
Obtains information on all partner systems which can be reached.

SELECT-PARAMETER = *PARAMETERS(PARTNER = <text 1..200 with-low>)
Obtains information on this partner system. You can specify the name from the partner list or the address of the partner system. The following information is supplied:

- if you are permitted to communicate with this partner system.
- the security level assigned to this partner system.
- if no authorization exists for the partner system, FTC0170 is displayed.

For additional information to partner addresses, see section “Defining partner properties” on page 44.

OUTPUT =
Output medium for the partner system listing.

OUTPUT = *SYSOUT(...)
The list is output on SYSOUT.

OUTPUT = *SYSLST(...)
The list is output on SYSLST.

LAYOUT = *STD
Output is put into a user-friendly form for reading.

LAYOUT = *CSV
Output is in **C**haracter **S**eparated **V**alues format. This is a special tabular format, widely used in the PC world, where the individual fields are separated by a semicolon “;“ (see section “Output in CSV format” on page 135).

Example

Steven Miller would like to find out about the security level of the computer BUYDACK. To do this, he uses the following command:

```
/SHOW-FT-RANGE␣SELECT-PARAMETER=(PARTNER=BUYDACK)
```

Short form:

```
/SHOW-FT-RANGE␣SEL=(BUYDACK)
```

He receives the following output:

```
%SECLEV  PARTNER-NAME
%  50    BUYDACK
```

The column SECLEV contains the security level of the partner system whose name appears in the PARTNER-NAME column.
If Steven had entered SELECT-PARAMETER=*ALL (or left out this parameter altogether), he would have received a similar but longer list of all accessible partner systems.

Command return codes

(SC2)	SC1	Maincode	Meaning
0	64	FTC0052	The output of information was interrupted.
0	0	FTC0054	There is no information which meets the specified criteria.
0	64	FTC0070	The command cannot be executed on the basis of inadequate operating resources.
0	64	FTC0152	The user ID entered is not the user’s own ID.
0	64	FTC0170	The partner entered is unknown within the partner systems possible for this user.
0	64	FTC0255	A system error occurred.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

OPS variables

Element	Type	Output
SEC-LEV	Integer	Security level
PARTNER-NAME	String	Partner name

5.38 START-FT Activate openFT

Note on usage

User group: FT administrator

Alias name: FTSTART

Functional description

The START-FT command is used to activate the specified openFT instance. If you have not selected another openFT instance using SET-FT-INSTANCE, then start the standard instance.

The command is only executed if openFT is not already active.

If the request queue contains file transfer requests for which the corresponding (remote) FT systems have also been started, these requests are started directly after openFT starts – provided the resources are available and no other start time has been defined.

It is possible to send SNMP traps, Console traps, and ADM traps on START-FT.

Adequate steps must also be taken to ensure that all pubsets are available. Otherwise locally submitted requests that require unavailable pubsets are terminated with an error message. If this happens, the user cannot be notified by a result list or job variable.

If, in BCAM, the BCMAP FUNCT=INIT command of the MAXMAP parameter is used, the command must be unconditionally created before starting openFT.

If the openFT instance is to run under a virtual host name, the virtual host name must first be entered using MODIFY-FT-OPTIONS before the START-FT.

Format

START-FT / FTSTART

Without operands

Correct execution of the START-FT command is acknowledged with the following message:

```
FTR0500 openFT 12.0A00 started. Protocols: openFT,FTAM, FTP, ADM
```

or

```
FTR0500 openFT 12.0A00 starting. Protocols: openFT,FTAM
```

(Here only the installied products or the activated protocols are displayed.)

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	*open*FT system activated. The SYSOUT message contains the *open*FT version as an insert.
83	32	CMD0221	Internal error.
1	0	FTR1020	Command rejected. *open*FT already started.
35	64	FTR1035	Command only permissible for FT administrator.
42	64	FTR1042	*open*FT could not be started.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

5.39 START-OPENFTPART List partner systems as command procedure

Note on usage

User group: FT administrator

Functional description

The START-OPENFTPART command can be used to have all partner systems listed as a command procedure. MODIFY-FT-PARTNER commands are generated. This procedure can then be used to back up and maintain the partner list.

Format

```
START-OPENFTPART

 OUTPUT = <filename>
,PARTNER = *ALL / <text 1..8>
```

Operands

OUTPUT = <filename>
Name of the file to be created.

PARTNER = *ALL
All partner systems are included in the command procedure.

PARTNER = <text 1..8>
Name of the partner system (or partner systems) that is to be included in the command procedure.
This entry may be specified as a unique partner name (1 - 8 alphanumeric characters) or as a group of partners (1 - 7 characters, which must end with an asterisk “∗”).

5.40 STOP-FT Deactivate openFT

Note on usage

User group: FT administrator

Alias name: FTSTOP

Functional description

The STOP-FT is used to initiate deactivation of the specified openFT instance and stop openFT.

The command is only executed if the instance has been started.

It is possible to send SNMP traps on STOP-FT.

Format

STOP-FT / FTSTOP

Without operands

Correct execution of the STOP-FT command is acknowledged with the following message:

```
%  FTR0501 openFT terminated
```

Command return codes

(SC2)	SC1	Maincode	Meaning
0	0	CMD0001	openFT system is terminated.
83	32	CMD0221	Internal error.
35	64	FTR1035	Command only permissible for FT administrator.
1	0	FTR1039	Command rejected. openFT is not active.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

Example

Activate the local openFT system and subsequently deactivate the FT system:

```
/START-FT
FTR0500 openFT 12.0A00 starting. Protocols: openFT,FTAM,FTP,ADM
.
.
/STOP-FT
FTR0501 openFT terminated
.
.
FTR0361 openFT control process terminated
```

Output from the console message FTR0361 can be controlled using MODIFY-FT-OPTIONS ...CONSOLE-TRAPS, e.g. with FT-STATE=*ON.

5.41 UPDATE-FT-PUBLIC-KEYS Update public keys

Note on usage

User group: FT administrator

Alias name: FTUPDKEY

Functional description

Using the UPDATE-FT-PUBLIC-KEYS command, you can newly create the public key files of the key pair sets present in your openFT instance. This may become necessary if the existing public key files are unintentionally deleted. In addition, the command imports updated comments from SYSPKF.COMMENT to the public key files (see below).

The key pair consists of a private key, which is administered internally by openFT, and a public key.

Public keys are stored on the configuration user ID of the openFT instance (default: $SYSFJAM) under the name:

SYSPKF.R<key reference>.L<key length>:

The key reference is a numeric designator for the version of the key pair. Following installation, the key length is 2048 bits by default. The public key files are text files that are created in the character code of the respective operating system, i.e. EBCDIC.DF04-1 for BS2000, IBM1047 for z/OS, ISO8859-1 for Unix systems and CP1252 for Windows systems.

In a file SYSPKF.COMMENT on the configuration user ID of the openFT instance / , you can store comments that are written in the first lines of this file when an existing public key file is updated. Such comments might contain, for example, the communications partner and the telephone number of the FT administrator on duty. The lines in the SYSPKF.COMMENT file may be a maximum of 78 characters in length.

Public key files with invalid key reference are automatically deleted (for example, public keys, for which openFT no longer has an internal private key).

Format

UPDATE**-FT-PUB**LIC**-KEYS** / **FTUPDKEY**

Without operands

Command return codes

(SC2)	SC1	Maincode	Meaning
83	32	CMD0221	Internal error.
33	64	FTR1033	The public key files could not be updated.
35	64	FTR1035	The user is not authorized to use this command.

SC1/2 = Subcode 1/2 in decimal notation
For additional information, see section “Command return codes” on page 133

6 Appendix

6.1 Structure of CSV outputs

6.1.1 Output format

The output format for all commands corresponds to the following rules:

- Each record is output in a separate line. A record contains all the information to be displayed on an object.
- The first line is a header and contains the field names of the respective columns. **Only the field names are guaranteed, not the order of fields in the record.** In other words, the order of columns is determined by the order of the field names in the header line.
- Two tables, with their own respective headers, are output sequentially for the command SHOW-FTAC-ENVIRONMENT. If one of the tables is empty, the corresponding header is also dropped.
- Individual fields within an output line are delimited by a semicolon “;”.

The following data types are differentiated in the output:

- Number

  Integer
- String
- String: Since ";" is a metacharacter in the CSV output, any text that contains ";" is enclosed in double quotes ("). Double quotes within a text field are doubled in order to differentiate them from text delimiters. When imported into a program, the doubled quotes are automatically removed and the text delimiters removed. Keywords are output in uppercase with a leading asterisk (*) and are not enclosed in double quotes.

- Date

  The date and time are output in the form yyyy-mm-dd hh:mm:ss. In some cases, only the short form yyyy-mm-dd is ouput, i.e. the date alone.

- Time

  The time is output in the form yyyy-mm-dd hh:mm:ss or only hh:mm:ss.

6.1.2 SHOW-FILE-TRANSFER

The following table indicates the CSV output format of a request.

Short output is also possible with SHOW-FILE-TRANSFER, see page 397.

The **Parameter** column contains the name of the output parameter during long output, see page 297.

Column	Type	Values and Meaning	Parameter
TransId	Number	Request ID	TRANSFER-ID
Initiator	String	*LOC / *REM Initiator is local / remote	INITIATOR
State	String	*LOCK / *WAIT / *HOLD / *FIN / *ACT / *CANC / *SUSP Request status	STATE
PartnerName	String	Name or address of the partner enclosed in double quotes	PARTNER
PartnerState	String	*ACT / *INACT / *NOCON / *INSTERR Partner status	PARTNER-STATE
TransDir	String	*TO / *FROM Transfer direction	TRANS
ByteNum	Number	Number of bytes transferred / empty	BYTECNT
LocFileName	String	File name or library name in the local system enclosed in double quotes	LOC: FILE or LIBRARY
LocElemName	String	Name of the library element in the local system enclosed in double quotes / *NSPEC	LOC: ELEMENT
LocElemType	String	Type of the library element in the local system enclosed in double quotes / *NSPEC / *NONE	LOC: TYPE
LocElemVersion	String	Version of the library element in the local system enclosed in double quotes / *NSPEC / *NONE	LOC: VERSION
Prio	String	*NORM / *LOW Priority of the request	PRIO
Compress	String	*NONE / *BYTE / *ZIP Compressed transfer	COMPRESS
DataEnc	String	*YES / *NO User data is transferred encrypted / unencrypted	ENCRYPT

Column	Type	Values and Meaning	Parameter
DiCheck	String	*YES / *NO Data integrity is checked / is not checked	DICHECK
Write	String	*REPL / *EXT / *NEW Write rules	WRITE
StartTime	String	Time at which the request is started (format yy-mm-dd hh:mm:ss) / *SOON (request is started as soon as possible)	START
CancelTime	String	Time at which the request is deleted from the request queue (format yy-mm-dd hh:mm:ss) / *NO (no delete time)	CANCEL
Owner	String	Local user ID enclosed in double quotes	OWNER
DataType	String	*CHAR / *BIN / *USER File type	DATA
Transp	String	*YES / *NO Transfer transparent / not transparent	TRANSP
LocTransAdmId	String	User ID for accessing the local system, enclosed in double quotes / *NONE	LOC: TRANS-ADM (USER)
LocTransAdmAcc	String	Account number for the local system / *NONE	LOC: TRANS-ADM=(...account)
LocProfile	String	Name of the admission profile for accessing the local system enclosed in double quotes / *NONE	LOC: TRANS-ADM=(profile)
LocProcAdmId	String	Transfer admission for follow-up processing in the local system enclosed in double quotes / *NONE	LOC: PROC-ADM=(user...)
LocProcAdmAcc	String	Account number for follow-up processing in the local system / *NONE	LOC: PROC-ADM=(...account)
LocSuccProc	String	Local follow-up processing on success, enclosed in double quotes / *NONE / *SECRET / empty	LOC: SUCC-PROC
LocFailProc	String	Local follow-up processing on error, enclosed in double quotes / *NONE / *SECRET / empty	LOC: FAIL-PROC
LocListing	String	*SYSLST / *LISTFILE / *NONE Result list in the local system	LOC: LIST
LocMonjv	String	Name of the job variable enclosed in double quotes / *NONE	LOC: MONJV
LocCcsn	String	Name of the character set in the local system enclosed in double quotes / *STD	LOC: CCSN

Column	**Type**	**Values and Meaning**	**Parameter**
RemFileName	String	File name in the remote system enclosed in double quotes / *NSPEC / *NONE / empty	REM: FILE or LIBRARY
RemElemName	String	Element name enclosed in double quotes / *NSPEC / *NONE	REM: ELEMENT
RemElemType	String	Element type enclosed in double quotes / *NSPEC / *NONE	REM: TYPE
RemElemVersion	String	Element version enclosed in double quotesn / *STD / *NONE	REM: VERSION
RemTransAdmId	String	User ID in the remote system enclosed in double quotes / *NONE	REM: TRANS-ADM=(user-id,...)
RemTransAdmAcc	String	Account number in the remote system enclosed in double quotes / empty	REM: TRANS-ADM=(...,account)
RemTransAdmAccount [1]	String	Account number in the remote system enclosed in double quotes / empty	REM: TRANS-ADM=(...,account)
RemProfile	String	*YES / *NONE *YES means access via FTAC admission profile	REM: TRANS-ADM=REMOTE-PROFILE
RemProcAdmId	String	Transfer admission for follow-up processing in the remote system enclosed in double quotes / *NONE	REM: PROC-ADM=(user-id,...)
RemProcAdmAcc	String	Account number for follow-up processing in the remote system enclosed in double quotes / *NONE	REM: PROC-ADM=(...,account)
RemSuccProc	String	Remote follow-up processing on success, enclosed in double quotes / *SECRET / *NONE / empty	REM: SUCC-PROC
RemFailProc	String	Remote follow-up processing on error, enclosed in double quotes / *SECRET / *NONE / empty	REM: FAIL-PROC
RemCcsn	String	Name of the character set used in the remote system, enclosed in double quotes / *STD	REM: CCSN
FileSize	Number	Size of the file in bytes / empty	FILESIZE
RecSize	Number	Maximum record size in bytes / empty	RECSIZE
RecFormat	String	*STD / *VARIABLE / *FIX / *UNDEFINED Record format	RECFORM
StoreTime	Date	Time at which the request was entered in the request queue	STORE

Column	Type	Values and Meaning	Parameter
ExpEndTime	Date	empty	---
TranspMode	String	*YES / *NO Transfer transparent / not transparent	TRANSP
DataEncrypt	String	*YES / *NO User data transferred encrypted / unencrypted	ENCRYPT
TabExp	String	*AUTO / *YES / *NO Tabulator expansion	TABEXP
Mail	String	*ALL / *FAIL / *NO Result messages	LOC: MAIL
DiagCode	String	empty	---
FileAvail	String	*IMMEDIATE / *DEFERRED / *NSPEC Availability (for FTAM only)	AVAILABILITY
StorageAccount	String	Account number (for FTAM only) / empty	STOR-ACCOUNT
AccessRights	String	FTAM access rights / empty Possible values are @r, @w or combinations of r, i, p, x, e, a, c, d	ACCESS-RIGHTS
LegalQualif	String	Legal qualification (for FTAM only) / empty	LEGAL-QUAL
PartnerPrio	String	*LOW / *NORM / *HIGH Partner priority	PARTNER-PRIO
TargetFileForm	String	*STD / *BLOCK / *SEQ File format in the target system	TARGFORM
TargetRecForm	String	*STD / *UNDEFINED Record format in the target system	TRECFRM
Protection	String	*STD / *SAME Transfer of protection attributes	PROTECT
GlobReqId	Number	Global request identification For locally issued requests, same as request ID; for globally issued requests, same as the request ID in the initiating system	TRANSFER-ID or GLOB-ID

[1] RemTransAdmAcc and RemTransAdmAccount have the same meaning and the same content. For reasons of compatibility, both parameters are present in the CSV output.

Short output from SHOW-FILE-TRANSFER in CSV format

INF=*SUMMARY outputs a table with two rows indicating the number of requests that have the corresponding status, see also page 289.

Column	Type	Values
Act	Number	Number of requests with the status ACTIVE
Wait	Number	Number of requests with the status WAIT
Lock	Number	Number of requests with the status LOCK
Susp	Number	Number of requests with the status SUSPEND
Hold	Number	Number of requests with the status HOLD
Fin	Number	Number of requests with the status FINISHED
Total	Number	Total number of requests

6.1.3 SHOW-FT-ADMISSION-SET

The following table indicates the CSV output format of an admission set.

The **Parameter** column contains the name of the output parameter during normal output, see page 308.

Column	Type	Values and Meaning	Parameter
UserId	String	User ID, enclosed in double quotes / *STD *STD means default admission set	USER-ID
UserMaxObs	Number	0 ... 100 Maximum user level for OUTBOUND-SEND	MAX. USER LEVELS OBS
UserMaxObsStd	String	*YES / *NO *YES means same value as default admission set [1]	
UserMaxObr	Number	0 ... 100 Maximum user level for OUTBOUND-RECEIVE	MAX. USER LEVELS OBR
UserMaxObrStd	String	*YES / *NO *YES means same value as default admission set[1]	
UserMaxIbs	Number	0 ... 100 Maximum user level for INBOUND-SEND	MAX. USER LEVELS IBS
UserMaxIbsStd	String	*YES / *NO *YES means same value as default admission set [1]	
UserMaxIbr	Number	0 ... 100 Maximum user level for INBOUND-RECEIVE	MAX. USER LEVELS IBR
UserMaxIbrStd	String	*YES / *NO *YES means same value as default admission set [1]	
UserMaxIbp	Number	0 ... 100 Maximum user level for INBOUND-PROCESSING	MAX. USER LEVELS IBP
UserMaxIbpStd	String	*YES / *NO *YES means same value as default admission set [1]	
UserMaxIbf	Number	0 ... 100 Maximum user level for INBOUND-FILE-MANAGEMENT	MAX. USER LEVELS IBF
UserMaxIbfStd	String	*YES / *NO *YES means same value as default admission set [1]	
AdmMaxObs	Number	0 ... 100 Maximum level of FTAC administrator for OUTBOUND-SEND	MAX. ADM LEVELS OBS
AdmMaxObsStd	String	*YES / *NO *YES means same value as default admission set [1]	

Column	Type	Values and Meaning	Parameter
AdmMaxObr	Number	0 ... 100 Maximum level of FTAC administrator for OUTBOUND-RECEIVE	MAX. ADM LEVELS OBR
AdmMaxObrStd	String	*YES / *NO *YES means same value as default admission set [1]	
AdmMaxIbs	Number	0 ... 100 Maximum level of FTAC administrator for INBOUND-SEND	MAX. ADM LEVELS IBS
AdmMaxIbsStd	String	*YES / *NO *YES means same value as default admission set [1]	
AdmMaxIbr	Number	0 ... 100 Maximum level of FTAC administrator for INBOUND-RECEIVE	MAX. ADM LEVELS IBR
AdmMaxIbrStd	String	*YES / *NO *YES means same value as default admission set [1]	
AdmMaxIbp	Number	0 ... 100 Maximum level of FTAC administrator for INBOUND-PROCESSING	MAX. ADM LEVELS IBP
AdmMaxIbpStd	String	*YES / *NO *YES means same value as default admission set [1]	
AdmMaxIbf	Number	0 ... 100 Maximum level of FTAC administrator for INBOUND-FILE-MANAGEMENT	MAX. ADM LEVELS IBF
AdmMaxIbfStd	String	*YES / *NO *YES means same value as default admission set [1]	
Priv	String	*YES / *NO *YES means admission set of FTAC administrator	ATTR
Password	String	*YES / *NO *YES means that an FTAC password has been defined	ATTR
AdmPriv	String	*NO	ATTR

[1] Relevant only if UserId is not *STD, *NO is always output in the case of the default admission set. In the normal output, *YES corresponds to an asterisk (*) after the value

6.1.4 SHOW-FT-KEY

The table below indicates the CSV format for the output of the properties of the RSA keys.

The **Parameter** column contains the name of the output parameter during normal output, see page 311.

Column	**Type**	**Values and Meaning**	**Parameter**
Reference	Number	Key reference	KEY-REF
Identification	String	Identification of the partner enclosed in double quotes / *OWN *OWN means the private key for the user’s own instance	IDENTIFICATION
PartnerName	String	Name of partner / *OWN *OWN means the private key for the user’s own instance	PARTNER
CreDate	Date	Date on which the key was generated	CRE-DATE
ExpDate	String	Date on which the key expires / *NONE	EXP-DATE
Expired	String	*YES / *NO Key has expired / not expired	EXP-DATE (EXPIRED)
KeyLen	Number	768 / 1024 / 2048 Key length in bits	KEY-LEN
AuthLev	Number	1 / 2 Authentication level	AUTHL

6.1.5 SHOW-FT-LOGGING-RECORDS

The following table indicates the CSV output format of a log record if the INF=*LOGGING-FILES has not been specified. If von INF=*LOGGING-FILES is specified then the output has a different format, see page 403.

The values that are indicated by an “x” in the **Std** column are also output if INF=*STD.

The **Parameter** column contains the name of the output parameter during long output, see page 328ff.

Column	Type	Values and Meaning	Parameter	Std
LogId	Number	Number of the log record (up to twelve digits)	LOGGING-ID	x
ReasonCode	String	Reason code enclosed in double quotes to prevent interpretation as a number. FTAC Reason Codes are output as hexadecimal strings	RC	x
LogTime	Date	Time at which the log record was written	TIME	x
InitUserId	String	Initiator of the request enclosed in double quotes / *REM	INITIATOR	x
InitTsn	String	TSN des Auftraggebers / *NONE	INITSN	x
PartnerName	String	Partner name enclosed in double quotes (name or address)	PARTNER	x
TransDir	String	*TO / *FROM / *NSPEC Transfer direction	TRANS	x
RecType	String	*FT / *FTAC / *ADM Type of log record	REC-TYPE	x
Func	String	*TRANS-FILE / *READ-FILE-ATTR / *DEL-FILE / *CRE-FILE / *MOD-FILE-ATTR / *READ-DIR / *MOVE-FILE / *CRE-FILE-DIR / *DEL-FILE-DIR / *LOGIN / *MOD-FILE-DIR / *REM-ADMIN FT function	FUNCTION	x
UserAdmisId	String	User ID to which the requests in the local system relate, enclosed in double quotes	USER-ADM	x
FileName	String	Local file name enclosed in double quotes	FILENAME	x
Priv	String	*YES / *NO / *NONE Profile is privileged / not privileged / not relevant because no profile was used or no FTAC log record is present	PRIV	
ProfName	String	Name of the FTAC profile enclosed in double quotes / *NONE	PROFILE	
ResultProcess	String	*STARTED / *NOT-STARTED / *NONE Status of follow-up processing	PCMD	

Column	Type	Values and Meaning	Parameter	Std
StartTime	Date	Start time of transfer	STARTTIME	
TransId	Number	Number of transfer request	TRANS-ID	
Write	String	*REPL / *EXT / *NEW / *NONE Write rules	WRITE	
StoreTime	Date	Acceptance time of request – If initiated in the local system: time the request was issued – If initiated in the remote system: time of entry in the request queueh	 REQUESTED STORETIME	
ByteNum	Number	Number of bytes transferred	TRANSFER	
DiagInf	String	Diagnostic information / *NONE	---	
ErrInfo	String	Additional information on the error message, enclosed in double quotes / *NONE	ERRINFO	
Protection	String	*SAME / *STD Protection attributes are transferred / not transferred	PROTECTION ---	
ChangeDate	String	*SAME / *STD Take over modification date of send file for receive file / do not take over modification date	CHG-DATE	
SecEncr	String	*YES / *NO Encryption of request description activated / deactivated	SEC-OPTS	
SecDichk	String	*YES / *NO Data integrity check of request description activated / deactivated	SEC-OPTS	
SecDencr	String	*YES / *NO Encryption of transferred file content activated / deactivated	SEC-OPTS	
SecDdichk	String	*YES / *NO Data integrity check of transferred file content activated / deactivated	SEC-OPTS	
SecLauth	String	*YES / *NO Authentication of the local system in the remote system activated / deactivated	SEC-OPTS	
SecRauth	String	*YES / *NO Authentication of the remote system in the local system activated / deactivated	SEC-OPTS	

Column	Type	Values and Meaning	Parameter	Std
RsaKeyLen	Number	768 / 1024 / 2048 / empty Length of the RSA key used for the encryptio in bit or empty if SecEncr does not have the value *YES	SEC-OPTS	
SymEncrAlg	String	*DES / *AES-128 / *AES-256 / empty The encryption algorithm used or empty if SecEncr does not have the value *YES	SEC-OPTS	
CcsName	String	Name of the character set enclosed in double quotes / empty	CCS-NAME	
AdminId	String	empty	ADMIN-ID	
Routing	String	Routing information enclosed in double quotes / empty	ROUTING	
AdmCmd	String	Administration kommand enclosed in double quotes / empty	ADM-CMD	
As3Type	String	empty (internal function)	---	
As3MsgTid	String	empty (internal function)	---	
As3RcpStat	String	empty (internal function)	---	
AuthLev	Number	1 / 2 / empty Authentication level	SEC-OPTS	
GlobReqId	Number	Global request identification (requests issued remotely) / empty (requests issued locally)	GLOB-ID	

CSV output on INF=*LOGGING-FILES

If the optionINF=*LOGGING-FILES is specified then only the following columns are output:

Column	Type	Values and Meaning	Parameter
TimeStamp	Date	Creation time of the log file	---
LoggingFileName	String	Fully qualified name of the log file	(file name)

6.1.6 SHOW-FT-MONITOR-VALUES

The following table shows the CSV output format for the monitoring values for openFT operation if all the monitoring values are output (NAME=*ALL,INF=*VALUES(..)).

If DATA=*RAW is specified, the duration values are not output (*Duxxx*, see footnote).

The default values are marked with "x" in the **Std** column. These are output if INF=*STD is specified.

For a detailed description of the monitoring values, refer to thesection “Description of the monitoring values” on page 343.

The individual monitoring values (ThNetbTtl ... StTrcr) have the same names in all the output formats (normal output, long output and CSV output).

Column	Type	Values prepared	Values not prepared	Meaning	Std
CurrTime	Date	Time	Time	Current timet	x
MonOn	Date	Time	Time	Start time of measurement date recording or last change of configuration (a modification of PartnerSel/ReqSel has the same effect as a new start)	x
PartnerSel	String6	*ALL / *NONE / OPENFT / FTAM / FTP		Partner type selected	x
ReqSel	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE		Request type selected	x
Data	String	FORM	RAW	Output format (perpared / not prepared)	x
ThNetbTtl	Number	Number of bytes per second	Bytes, accumulated	Throughput in net bytes	x
ThNetbSnd	Number	Number of bytes per second	Bytes, accumulated	Throughput in net bytes, send requests	x
ThNetbRcv	Number	Number of bytes per second	Bytes, accumulated	Throughput in net bytes, receive requests	x
ThNetbTxt	Number	Number of bytes per second	Bytes, accumulated	Throughput in net bytes, text files	
ThNetbBin	Number	Number of bytes per second	Bytes, accumulated	Throughput in net bytes, binary files	
ThDiskTtl	Number	Number of bytes per second	Bytes, accumulated	Throughput in disk bytes	x
ThDiskSnd	Number	Number of bytes per second	Bytes, accumulated	Throughput in disk bytes, send requests	x

Column	Type	Values prepared	Values not prepared	Meaning	Std
ThDiskRcv	Number	Number of bytes per second	Bytes, accumulated	Throughput in disk bytes, receive requests	x
ThDiskTxt	Number	Number of bytes per second	Bytes, accumulated	Throughput in disk bytes, text files	
ThDiskBin	Number	Number of bytes per second	Bytes, accumulated	Throughput in disk bytes, binary files	
ThRqto	Number	Number per second	Number, accumulated	openFT requests received	x
ThRqft	Number	Number per second	Number, accumulated	File transfer requests received	
ThRqfm	Number	Number per second	Number, accumulated	file management requests received	
ThSuct	Number	Number per second	Number, accumulated	Successfully completed openFT requests	x
ThAbrt	Number	Number per second	Number, accumulated	Aborted openFT requests	x
ThIntr	Number	Number per second	Number, accumulated	Interrupted openFT requests	x
ThUsrf	Number	Number per second	Number, accumulated	Requests from non-authorized users	x
ThFoll	Number	Number per second	Number, accumulated	Follow-up processing operations started	
ThCosu	Number	Number per second	Number, accumulated	Connections established	
ThCofl	Number	Number per second	Number, accumulated	Failed connection attempts	x
ThCobr	Number	Number per second	Number, accumulated	Disconnections as a result of connection errors	x
DuRqtlOut[1]	Number	Milliseconds	---	Maximum request duration Outbound	
DuRqtlInb[1]	Number	Milliseconds	---	Maximum request duration Inbound	
DuRqftOut[1]	Number	Milliseconds	---	Maximum request duration Outbound transfer	
DuRqftInb[1]	Number	Milliseconds	---	Maximum request duration Intbound transfer	
DuRqfmOut[1]	Number	Milliseconds	---	Maximum request duration Outbound file management	

Column	**Type**	**Values prepared**	**Values not prepared**	**Meaning**	**Std**
DuRqfmInb[1]	Number	Milliseconds	---	Maximum request duration Inbound file management	
DuRqesOut[1]	Number	Milliseconds	---	Maximum outbound request waiting time	
DuDnscOut[1]	Number	Milliseconds	---	Maximum time an outbound openFT request was waiting for partner checking	
DuDnscInb[1]	Number	Milliseconds	---	Maximum time an inbound openFT request was waiting for partner checking	
DuConnOut[1]	Number	Milliseconds	---	Maximum duration tim of establishment of a connection for an outbound openFT request	
DuOpenOut[1]	Number	Milliseconds	---	Maximum file open time (outbound)	
DuOpenInb[1]	Number	Milliseconds	---	Maximum file open time (inbound)	
DuClosOut[1]	Number	Milliseconds	---	Maximum file close time (outbound)	
DuClosInb[1]	Number	Milliseconds	---	Maximum file close time (inbound)	
DuUsrcOut[1]	Number	Milliseconds	---	Maximum user check time (outbound)	
DuUsrcInb[1]	Number	Milliseconds	---	Maximum user check time (ínbound)	
StRqas	Number (100)[2]	Average value	Current number	Number of synchronous requests in the ACTIVE state	x
StRqaa	Number (100)[2]	Average value	Current number	Number of asynchronous requests in the ACTIVE state	x
StRqwt	Number (100)[2]	Average value	Current number	Number of requests in the WAIT state	x
StRqhd	Number (100)[2]	Average value	Current number	Number of requests in the HOLD state	x
StRqsp	Number (100)[2]	Average value	Current number	Number of requests in the SUSPEND state	x
StRqlk	Number (100)[2]	Average value	Current number	Number of requests in the LOCKED state	x
StRqfi	Number (100)[2]	Average value	Current number	Number of requests in the FINISHED state	

Column	Type	Values prepared	Values not prepared	Meaning	Std
StCLim	Number	Value currently set		Maximum number of connections established for asynchronous requests.	x
StCAct	Percent	Share of StCLim in %	Current number	Number of occupied connections for asynchronous requests	x
StRqLim	Number	Value currently set		Maximum number of asynchronous requests in request management	x
StRqAct	Percent	Share of StRqLim in %	Current number	Entries occupied in request management	x
StOftr	BOOL	1 / 0		openFT Protocol activated / deactivated	x
StFtmr	BOOL	1 / 0		FTAM Protocol activated / deactivated	x
StFtpr	BOOL	1 / 0		FTP Protocol activated / deactivated	x
StTrcr	BOOL	1 / 0		Trace activated / deactivated	

[1] is not output with DATA=*RAW

[2] number is the measured value multiplied by 100 (e.g. output 225 corresponds to value 2.25)

Examples

```
/SHOW-FT-MONITOR-VALUES NAME=*ALL,OUTPUT=*SYSOUT(*CSV)
```

```
CurrTime;MonOn;PartnerSel;ReqSel;Data;ThNetbTtl;ThNetbSnd;ThNetbRcv;ThNetbTxt
;ThNetbBin;ThDiskTtl;ThDiskSnd;ThDiskRcv;ThDiskTxt;ThDiskBin;ThRqto;ThRqft;Th
Rqfm;ThSuct;ThAbrt;ThIntr;ThUsrf;ThFoll;ThCosu;ThCofl;ThCobr;DuRqtlOut;DuRqtl
Inb;DuRqftOut;DuRqftInb;DuRqfmOut;DuRqfmInb;DuRqesOut;DuDnscOut;DuDnscInb;DuC
onnOut;DuOpenOut;DuOpenInb;DuClosOut;DuClosInb;DuUsrcOut;DuUsrcInb;StRqas;StR
qaa;StRqwt;StRqhd;StRqsp;StRqlk;StRqfi;StCLim;StCAct;StRqLim;StRqAct;StOftr;S
tFtmr;StFtpr;StTrcr
```

```
2012-07-13 10:44:24;2012-07-13 10:35:46;*ALL;*ALL;FORM;0;0;0;0;0;0;0;0;0;
0;0;0;0;0;0;0;0;0;0;0;0;5129;0;5129;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;0;1
6;0;2000;0;1;0;1;0
```

6.1.7 SHOW-FT-OPTIONS

The following table indicates the CSV output format of the operating parameters

The **Parameter** column contains the name of the output parameter during normal output, see page 358ff. Some parameters have fixed values because they are supported only for reasons of compatibility or have been replaced by other parameters.

Column	Type	Values and Meaning	Parameter
PartnerLim	Number	0	---
ReqLim	Number	Maximum number of requests	RQ-LIM
TaskLim	Number	Maximum number of processes	PROC-LIM
ConnLim	Number	Maximum number of connections	CONN-LIM
ReqWaitLev	Number	1	---
TransportUnitSize	Number	Maximum length of a transport unit	TU-SIZE
PartnerCheck	String	*STD / *TRANSP-ADDR Partner check	PTN-CHK
SecLev	Number	0... 100 / *B-P-ATTR Default value for the security level of partners	SEC-LEV
TraceOpenft	String	*STD / *OFF Trace function for openFT partner activated / deactivated	FUNCT, line TRACE PARTNER-SELECTION
TraceOut	String	empty	FUNCT, line TRACE SWITCH---
TraceSession	String	*OFF	---
TraceFtam	String	*STD / *OFF Trace function for FTAM partner activated / deactivated	FUNCT, line TRACE PARTNER-SELECTION
LogTransFile	String	*ON / *OFF FT logging activated / deactivated	FT-LOG
MaxInboundReq	Number	Maximum number of requests	(same as RQ-LIM)
MaxReqLifetime	String	Maximum lifetime of requests in the request queue / *UNLIMITED	MAX-RQ-LIFE
SnmpTrapsSubsystemState	String	*ON / *OFF SNMP traps on subsystem status change activated / deactivated	TRAP, line SNMP SS-STATE
SnmpTrapsFtState	String	*ON / *OFF SNMP traps on asynchronous server status change activated / deactivated	TRAP, line SNMP FT-STATE

Column	Type	Values and Meaning	Parameter
SnmpTrapsPartnerState	String	*ON / *OFF SNMP traps on partner status change activated / deactivated	TRAP, line SNMP PART-STATE
SnmpTrapsPartnerUnreach	String	*ON / *OFF SNMP traps on unreachable partner systems activated / deactivated	TRAP, line SNMP PART-UNREA
SnmpTrapsReqQueueState	String	*ON / *OFF SNMP traps on request management status change activated / deactivated	TRAP, line SNMP RQ-STATE
SnmpTrapsTransSucc	String	*ON / *OFF SNMP traps on successfully terminated requests activated / deactivated	TRAP, line SNMP TRANS-SUCC
SnmpTrapsTransFail	String	*ON / *OFF SNMP traps on failed requests activated / deactivated	TRAP, line SNMP TRANS-FAIL
ConsoleTraps	String	*ON / *OFF Console traps (for at least one criterion) activated / deactivated.	TRAP, line CONS
TeleService	String	empty	
HostName	String	Host name of the local computer / *NONE	HOST-NAME
Identification	String	Instance identification enclosed in double quotes	IDENTIFICATION
UseTns	String	*NO	---
ConsTrapsSubsystemState	String	*ON / *OFF Console traps on subsystem status change activated / deactivated	TRAP, line CONS SS-STATE
ConsTrapsFtState	String	*ON / *OFF Console traps on asynchronous server status change activated / deactivated	TRAP, line CONS FT-STATE
ConsTrapsPartnerState	String	*ON / *OFF Console traps on partner status change activated / deactivated	TRAP, line CONS PART-STATE
ConsTrapsPartnerUnreach	String	*ON / *OFF Console traps on unreachable partner systems activated / deactivated	TRAP, line CONS PART-UNREA
ConsTrapsReqQueueState	String	*ON / *OFF Console traps on request management status change activated / deactivated	TRAP, line CONS RQ-STATE

Column	Type	Values and Meaning	Parameter
ConsTrapsTransSucc	String	*ON / *OFF Console traps on successfully terminated requests activated / deactivated	TRAP, line CONS TRANS-SUCC
ConsTrapsTransFail	String	*ON / *OFF Console traps on failed requests activated / deactivated	TRAP, line CONS TRANS-FAIL
FtLog	String	*ALL / *FAIL / *NONE Scope of FT logging	FT-LOG
FtacLog	String	*ALL / *FAIL / *NONE Scope of FTAC logging	FTAC-LOG
Trace	String	*ON / *OFF Trace function activated / deactivated	FUNCT, line TRACE SWITCH
TraceSelp	String	*ALL / OPENFT / FTP / FTAM / ADM / empty [1] Trace selection based on partner type	FUNCT, line TRACE PARTNER-SELECTION
TraceSelr	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE [1] Trace selection based on request type	FUNCT, line TRACE REQUEST-SELECTION
TraceOpt	String	*NO-BULK-DATA / *NONE Minimum trace / no trace options	FUNCT, line TRACE OPTIONS
KeyLen	Number	768 / 1024 / 2048 RSA key length in bit	KEY-LEN
CcsName	String	empty	---
AppEntTitle	String	*YES In the case of FTAM, "nil-Application Entity Title" is sent	---
StatName	String	$FJAM	---
SysName	String	Name of the local system (host name)	---
FtStarted	String	*YES / *NO openFT started / not started	STARTED
openftAppl	String	*STD / port number Port number of the local openFT server	OPENFT-APPL
ftamAppl	String	*STD / port number Port number of the local FTAM server	FTAM-APPL
FtpPort	Number	Port number Port number of the local FTP server	FTP-PORT
ftpDPort	Number	Value / empty (internal function)	---
ftstdPort	String	*STD / port number Default port for dynamic partners	---

Column	**Type**	**Values and Meaning**	**Parameter**
DynPartner	String	*ON / *OFF Dynamic partner entries activated / deactivated	DYN-PART
ConTimeout	Number	Value (internal function)	---
ChkpTime	Number	Value (internal function)	---
Monitoring	String	*ON / *OFF Monitoring data activated / deactivated	FUNCT, line MONITOR SWITCH
MonSelp	String	*ALL / OPENFT / FTP / FTAM / empty [1] Selection based on type of partner system	FUNCT, line MONITOR PARTNER-SELECTION
MonSelr	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE [1] Selection based on type of request	FUNCT, line MONITOR REQUEST-SELECTION
AdmTrapServer	String	Name of the ADM-TRAP server / *NONE	ADM-TRAP-SERVER
AdmTrapsFtState	String	*ON / *OFF ADM traps on asynchronous server status change activated / deactivated	TRAP, line ADM FT-STATE
AdmTrapsPartnerState	String	*ON / *OFF ADM traps on partner status change activated / deactivated	TRAP, line ADM PART-STATE
AdmTrapsPartnerUnreach	String	*ON / *OFF ADM traps on unreachable partner systems activated / deactivated	TRAP, line ADM PART-UNREA
AdmTrapsReqQueueState	String	*ON / *OFF ADM traps on request management status change activated / deactivated	TRAP, line ADM RQ-STATE
AdmTrapsTransSucc	String	*ON / *OFF ADM traps on successfully terminated requests activated / deactivated	TRAP, line ADM TRANS-SUCC
AdmTrapsTransFail	String	*ON / *OFF ADM traps on failed requests activated / deactivated	TRAP, line ADM TRANS-FAIL
AdminConnLim	String	Maximum number of administration connections	ADM-CLIM
AdmPort	String	Port number / *NONE Port number for remote administration	ADM-PORT
OpenftApplState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status of the openFT server	OPENFT-APPL, 2nd line
FtamApplState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status of the FTAM server	FTAM-APPL, 2nd line

Column	**Type**	**Values and Meaning**	**Parameter**
FtpState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status of the FTP server	FTP-PORT, 2nd line
AdmState	String	*ACTIVE / *INACT / *DISABLED Status for inbound remote administration	ADM-PORT, 2nd line
AdminLog	String	*ALL / *FAIL / *MODIFY / *NONE Scope of ADM logging	ADM-LOG
CentralAdminServer	String	*NO	---
ActiveAppl	String	*ALL / *NONE / OPENFT / FTAM / FTP / ADM[1] active servers	see 2nd line of OPENFT-APPL, FTAM-APPL, FTP-PORT, ADM-PORT
UseCmx	String	*NO	---
TraceOptLowerLayers	String	*OFF	---
EncMandIn	String	*YES / *NO Inbound encryption activated / deactivated	ENC-MAND (IN)
EncMandOut	String	*YES / *NO Outbound encryption activated / deactivated	ENC-MAND (OUT)
DelLog	String	*ON / *OFF Automatic deletion of log records activated / deactivated	DEL-LOG
DelLogRetpd	Number	Minimum age, in days, of the log records to be deleted. 0 means current day.	RETPD
DelLogRepeat	String	*MONTHLY / *WEEKLY / *DAILY Repeat interval for deletion of log records.	DEL-LOG ON
DelLogDay	Number	1..31 / 1..7 / 0 Day on which deletion is to be repeated. In the case of DelLogRepeat = *MONTHLY then this is the day of the month, if DelLogRepeat = *WEEKLY then it is the day of the week (1 = Monday), if DelLogRepeat = *DAILY then 0 is output	DEL-LOG ON
DelLogTime	Time	Time of deletion	DEL-LOG AT

[1] Combinations of multiple values are also possible (not with *ALL or *NONE)

6.1.8 SHOW-FT-PARTNERS

The following table indicates the CSV output format of a partner in the partner list.

The **Parameter** column contains the name of the output parameter during long output, see page 367.

Column	Type	Values and Meaning	Parameter
PartnerName	String	Partner name enclosed in double quotes	NAME
Sta	String	*ACT / *DEACT / *NOCON / *LUNK / *RUNK / *ADEAC / *AINAC / *LAUTH / *RAUTH / *NOKEY / *DIERR / *IDREJ Partner status	STATE
SecLev	String	*STD / *B-P-ATTR / 1...100 Global security level / attribute-specific security level / fixed security level	SECLEV
Trace	String	*FTOPT / *STD / *ON / *OFF Trace setting	TRACE
Loc	Number	Number of locally issued file transfer requests to this partner	LOC
Rem	Number	Number of file transfer requests issued by this partner	REM
Processor	String	empty	---
Entity	String	empty	---
NetworkAddr	String	Partner address (network address without port number/selectors) enclosed in double quotes	ADDRESS
Port	Number	Port number	ADDRESS (port number)
PartnerCheck	String	*FTOPT / *STD / *TRANSP-ADDR / *AUTH / *AUTHM / *NOKEY Sender verification	P-CHK
TransportSel	String	Transport selector enclosed in double quotes / empty	ADDRESS (transport selector)
LastAccessDate	Date	Time of last access in short format yyyy-mm-dd	---
SessionSel	String	Session selector enclosed in double quotes / empty	ADDRESS (session selector)
PresentationSel	String	Presentation selector enclosed in double quotes / empty	ADDRESS (presentation selector)
Identification	String	Identification enclosed in double quotes / empty	IDENTIFICATION

Column	Type	Values and Meaning	Parameter
SessRout	String	Routing information enclosed in double quotes / *ID / empty *ID means routing information same as identification	ROUTING
PartnerAddr	String	Partner address (including port number und selectors) enclosed in double quotes	ADDRESS
Check	String	*FTOPT / *STD / *TRANSP-ADDR Partner check	P-CHK
AuthMand	String	*YES / *NO Authentication is mandatory / not mandatory	P-CHK
Priority	String	*LOW / *NORM / *HIGH Priority	PRI
AS3	String	*NO (internal function)	---
AuthLev	Number	1 / 2 / empty Authentication level	P-CHK
InboundSta	String	*ACT / *DEACT Inbound function activated / deactivated	INBND
RequProc	String	*STD / *SERIAL The processing mode for asynchronous outbound requests is parallel / is serial	REQU-P

6.1.9 SHOW-FT-PROFILE

The following table indicates the CSV output format of an admission profile.

The values that are marked by an “x” in the **Std** column are also output if INF=*ONLY-NAMES is specified.

The **Parameter** column contains the name of the output parameter during long output, see also page 377f.

Column	Type	Values and Meaning	Parameter	Std
ProfName	String	Name of the profile enclosed in double quotes	(Profile name)	x
Priv	String	*YES / *NO Profile is privileged / not privileged	PRIVILEGED	x
TransAdm	String	*SECRET / *NSPEC Transfer admission has been assigned / not assigned	TRANS-ADM NOT-SPECIFIED	x
Duplicated	String	*YES / *NO *YES means: profile is locked due to attempt to assign the transfer admission twice	TRANS-ADM DUPLICATED	x
LockedByImport	String	*YES / *NO *YES means: profile is locked because it was imported	TRANS-ADM LOCKED (by_import)	x
LockedByAdm	String	*YES / *NO *YES means: profile locked by FTAC administrator	TRANS-ADM LOCKED (by_adm)	x
LockedByUser	String	*YES / *NO *YES means: profile locked by user	TRANS-ADM LOCKED (by_user)	x
Expired	String	*YES / *NO *YES means: profile locked because period expired	TRANS-ADM EXPIRED	x
ExpDate	String	Expiration date in short format yyyy-mm-dd / *NRES (no expiration date)	EXP-DATE	
Usage	String	*PUBLIC / *PRIVATE / *NSPEC Usage	USAGE	
IgnObs	String	*YES / *NO Ignore / do not ignore predefined value for Outbound Send	IGN-MAX-LEVELS OBS	
IgnObr	String	*YES / *NO Ignore / do not ignore predefined value for Outbound Receive	IGN-MAX-LEVELS OBR	

Column	Type	Values and Meaning	Parameter	Std
IgnIbs	String	*YES / *NO Ignore / do not ignore predefined value for Inbound Send	IGN-MAX-LEVELS IBS	
IgnIbr	String	*YES / *NO Ignore / do not ignore predefined value for Intbound Receive	IGN-MAX-LEVELS IBR	
IgnIbp	String	*YES / *NO Ignore / do not ignore predefined value for Inbound Processing	IGN-MAX-LEVELS IBP	
IgnIbf	String	*YES / *NO Ignore / do not ignore predefined value for Inbound File Management	IGN-MAX-LEVELS IBF	
Initiator	String	*LOC / *REM / *NRES Initiator: only local / only remote / unrestricted	INITIATOR	
TransDir	String	*FROM / *TO / *NRES Permitted transfer direction: from partner / to partner / unrestricted	TRANS-DIR	
MaxPartLev	Number	0... 100 / *NRES Maximum security level / security level unrestrictedt	MAX-PART-LEV	
Partners	String	One or more FT partners, delimited by commas and enclosed in double quotes / *NRES (no restriction)	PARTNER	
FileName	String	File name or file name prefix enclosed in double quotes / *NRES Restricts access to this file or files with this prefix. *NRES means there is no restriction	FILE-NAME	
Library	String	Library name enclosed in double quotes / *YES / *NO / *NRES Restricts access to this library, *NRES means there is no restriction	LIBRARY	
FileNamePrefix	String	*YES / *NO The file name in FileName is a prefix / is not a prefix	FILE-NAME = (PREFIX=..)	
ElemName	String	Name of the library element enclosed in double quotes / *NONE / *NRES	ELEMENT	
ElemPrefix	String	*YES / *NO The element name in ElemName is a prefix / is not a prefix	ELEMENT	

Column	**Type**	**Values and Meaning**	**Parameter**	**Std**
ElemVersion	String	Version of the library element enclosed in double quotes / *STD / *NONE / *NRES	ELEMENT	
ElemType	String	Type of the library element enclosed in double quotes / *NONE / *NRES	TYPE	
FilePass	String	*YES / *NRES / *NONE File password	---	
Write	String	*NEW / *EXT / *REPL / *NRES Write rules	WRITE	
UserAdmId	String	User ID enclosed in double quotes	USER-ADM (user-id,...)	x
UserAdmAcc	String	Account number enclosed in double quotes / *FIRST/ *NSPEC / *NRES / *NONE	USER-ADM (..,account,...)	
UserAdmPass	String	*OWN / *YES / *NSPEC / *NONE Password is taken over / was specified / was not specified / is not required	USER-ADM (...,...,password)	
ProcAdmId	String	User ID used for follow-up processing, enclosed in double quotes / *SAME / *NRES	PROC-ADM (user-id,...)	
ProcAdmAcc	String	Account number used for follow-up processing, enclosed in double quotes / *SAME / *NRES / *NONE	PROC-ADM (..,account,...)	
ProcAdmPass	String	*NONE / *YES / *SAME / *NRES Password is taken over / was specified / was not specified /is not required	USER-ADM (...,...,password)	
SuccProc	String	Follow-up processing on success, enclosed in double quotes / *NONE / *NRES / *EXPANSION	SUCC-PROC	
SuccPrefix	String	Folow-up processing prefix on success, enclosed in double quotes / *NONE	SUCC-PREFIX	
SuccSuffix	String	Follow-up processing suffix on success, enclosed in double quotes / *NONE	SUCC-SUFFIX	
FailProc	String	Follow-up processing on error, enclosed in double quotes / *NONE / *NRES / *EXPANSION	FAIL-PROC	
FailPrefix	String	Follow-up processing prefix on error, enclosed in double quotes / *NONE	FAIL-PREFIX	
FailSuffix	String	Follow-up processing suffix on error, enclosed in double quotes / *NONE	FAIL-SUFFIX	

Column	Type	Values and Meaning	Parameter	Std
TransFile	String	*ALLOWED / *NOT-ALLOWED Transfer and delete files permitted / not permitted	FT-FUNCTION = (TRANSFER-FILE)	
ModFileAttr	String	*ALLOWED / *NOT-ALLOWED Modify file attributes permitted / not permitted	FT-FUNCTION = (MODIFY-FILE-ATTRIBUTES)	
ReadDir	String	*ALLOWED / *NOT-ALLOWED View directories permitted / not permitted	FT-FUNCTION = (READ-DIRECTORY)	
FileProc	String	*ALLOWED / *NOT-ALLOWED Preprocessing/postprocessing permitted / not permitted	FT-FUNCTION = (FILE-PROCESSING)	
AccAdm	String	*NOT-ALLOWED	---	
RemAdm	String	*ALLOWED / *NOT-ALLOWED Remote administration via remote administration server permitted / not permitted	FT-FUNCTION = (REMOTE-ADMINISTRATION)	
Text	String	Text enclosed in double quotes / *NONE	TEXT	
DataEnc	String	*YES / *NO / *NRES Data encryption is mandatory / prohibited / neither mandatory nor prohibited	DATA-ENC	
ModDate	Date	Time of last modification	LAST-MODIF	
AdmTrapLog	String	*ALLOWED / *NOT-ALLOWED Reception of ADM traps permitted / not permitted	FT-FUNCTION = (ADM-TRAP-LOG)	

6.1.10 SHOW-FT-RANGE

The following table indicates the CSV output format of partners.

The **Parameter** column contains the name of the output parameter during normal output, see page 382.

Column	Type	Values and Meaning	Parameter
SecLev	Number	Security level	SECLEV
PartnerName	String	Partner name	PARTNER-NAME

6.1.11 SHOW-FTAC-ENVIRONMENT

The command SHOW-FTAC-ENVIRONMENT sequentially displays the objects contained in an FTAC export file in a format that corresponds to the output of the SHOW-FT-ADMISSION-SET (page 398) and SHOW-FT-PROFILE (page 415) commands.

6.2 Accounting records

Structure of the FT accounting records

The FT accounting record is divided into four parts:

1. record definition
2. identification section
3. basic information
4. variable information

The record sections contain the displacement, length and format of the data field.

The **field number** identifies the sequence number within the part of the record written.

The **displacement** is the position of the data field relative to the beginning of the part of the record that has been written.

The **length** is the length of the data field in bytes.

The **format** is the format of the data field:

A = alphanumeric (including $, #, and @)

B = binary number

C = printable characters

F = file name for BS2000

Z = unpacked decimal number (0...9)

– = undefined

1. Record definition section

The record definition section contains the record identifier, the time of day, the length of the identification section and the length of the basic information.

Field No.	Displ.	Length	Format	Meaning
1	00	4	A	Record identifier ‘FTR0‘
2	04	8	- /B	Time stamp of the time-of-day clock
3	0C	2	B	Length of the identification section
4	0E	2	B	Length of the basic information
5	10	4	-	Reserved

Layout of the record definition section

2. Identification section

The identification section contains the user ID, account number and job number (TSN).

Field No.	Displ.	Length	Format	Meaning
1	00	8	A	User ID
2	08	8	A	Account number
3	10	4	Z	Job number (TSN) (This field applies only to locally issued requests.)

Layout of the identification section

3. Basic information

The basic information includes

- Date and time when the FT request was stored,
- Date and time when the transfer ended,
- Result of the transfer,
- Details of the start of follow-up processing,
- Name of the remote system,
- Indication as to whether the accounting record was written by the local or the remote system,
- Identification of the FT request,
- Number of disk accesses,
- Number of bytes written to or read from disk,
- Number of bytes sent to or read from the accounting record.

Field No.	Displ.	Length	Format	Meaning
1	00	12	Z	Time when the file transfer request was stored (format: yymmddhhmmss; this field applies only to locally issued requests)
2	0C	12	Z	Time when the transfer ended (format: yymmddhhmmss)
3	18	1	C	Result of the transfer: + : successful execution - : execution with errors 0 : not used
4	19	1	C	Result of the start of follow-up: + : successful execution - : execution with errors 0 : not used
5	1A	8	A	Partner name
6	22	1	A	Specifies whether the request was issued in local or remote system: L : the request was submitted in the local system R : the request was submitted in the remote system
7	23	11	Z	Transfer ID
8	2E	2	-	Reserved
9	30	4	-	Reserved

Layout of the basic information

Field No.	Displ.	Length	Format	Meaning
10	34	4	B	Number of disk accesses
11	38	8	B	Number of bytes on disk
12	40	8	B	Number of bytes in network

Layout of the basic information

4. Variable information

Field No.	Displ.	Length	Format	Meaning
1	00	2	B	Number of extensions = 4
2	02	2	B	Displacement of the record extension for the file name from the start of record
3	04	2	B	Displacement of the record extension for the library member name from the start of record
4	06	2	B	Displacement of the record extension for the century part of the time specification from the start of the record
5	08	2	B	Displacement of the record extension for the CPU time from the start of the record
The variable information includes the file name and the name of the library member.				

Header of the variable section

Field No.	Displ.	Length	Format	Meaning
1	00	2	A	Extension identification = ‘FN‘
2	02	1	B	Extension type = x‘00‘
3	03	1	B	Length of the file name
4	04	see field 3	F	File name
If a displacement is set to 0, the corresponding record extension has not been specified.				

Record extension for the file name

Field No.	Displ.	Length	Format	Meaning
1	00	2	A	Extension identification = ‘MN‘
2	02	1	B	Extension type = x‘00‘
3	03	1	B	Length of extension (not including identification, type and length field)
4	04	8	A	Library member type
5	0C	24	A	Library member version
6	24	8	Z	Library member variant
7	2C	1	B	Length of library member name
8	2D	see field 7	A	Library member name

Record extension for the library member name

Field No.	Displ.	Length	Format	Meaning
1	00	2	A	Extension identification = ‘YY‘
2	02	1	B	Extension type = x‘00‘
3	03	1	B	Length of extension (not including identification, type, length field) = 4
4	04	2	Z	Time at which the request was stored in the form yy (see field 1 in the basic information)
5	06	2	Z	Time of transfer in the form yy (see field 2 in basic information)

Record extension for the century part of the time specification

Field No.	Displ.	Length	Format	Meaning
1	00	2	A	Extension identification = ‘MS‘
2	02	1	B	Extension type = x‘00‘
3	03	1	B	Length of extension (not including identification, type, length field) = 4
4	04	4	B	Number of machine commands required in the local system by this request (in units of 10,000 commands)

Record extension for CPU time

6.3 Recovering from hung FT and FTAC subsystems

In some cases, e.g. when system errors occur, it may not be possible to unload the subsystems. This may be due to the following reasons:

– The subsystem is in a LOCKED state, since the associated holder task can no longer be used, e.g. after a system dump.

– The subsystem cannot be unloaded because some tasks are still connected. This typically occurs when FT cannot be exited (the tasks with the TSNs FTC* and the FT server tasks (job name FTSP) do not disappear) when connected tasks enter permanent wait states, or when tasks are “permanently pending” after system dumps due to insufficient disk space.

In such exceptional cases, the system administrator can resort to some special resources to unload the subsystems and thus save the BS2000 session. These resources are described in the DSSM manual. The following points discuss some of the aspects to be observed when unloading the FT subsystems.

⚠ **WARNING!**

There is always a certain risk involved in using any such resources. There is essentially no way of guaranteeing that all error states are fully described here. The ultimate responsibility always lies with the system administrator !

A subsystem in a LOCKED state can be removed from the system by using the command /UNLOCK-SUBSYSTEM. Note, however, that this does **not** call the subsystem-specific uninstallation routine and therefore has the following consequences for the FT subsystem:

● No file locks held by FT are released, so all user files locked by FT will remain locked. These locks can be removed explicitly by the system administrator with VERIFY or will disappear implicitly at the next BS2000 startup.

A subsystem to which tasks are still connected can be unloaded with /STOP-SUBSYSTEM FORCE=YES if required, provided the attribute FORCED=ALLOWED is first assigned with the command /MOD-SUBSYSTEM-PARAMETERS. By default, FT subsystems do not have this attribute.

This approach causes any restarted tasks that are still connected to run with a system dump. Such system dumps are of no use whatsoever for any diagnostic purposes and may hence be discarded. FT tasks which are still connected and which are stuck in a bourse will run within at most 10 minutes of the system dump.

The subsystem should never be restarted as long as there are existing tasks which were still connected at the time of forcing the subsystems to unload!

Glossary

Italic type indicates a reference to other terms in this glossary.

access control
File attribute in the *virtual filestore*, attribute of the *security group* that defines *access rights*.

access protection
Comprises all the methods used to protect a data processing system against unauthorized system access.

access right / access admission
Derived from the *transfer admission*. The access right defines the scope of access for the user who specifies the transfer admission.

action list
Component of the file attribute *access control* (attribute of the *security group*) in the *virtual filestore* that defines *access rights*.

ADM administrator
Administrator of the *remote administration server*. This is the only person permitted to modify the configuration data of the remote administration server.

ADM partner
Partner system of an openFT instance with which communication takes place over the *FTADM protocol* in order to perform *remote administration*.

ADM traps
Short messages sent to the *ADM trap server* if certain events occur during operation of openFT.

ADM trap server
Server that receives and permanently stores the *ADM traps*. It must be configured as a *remote administration server*.

administrated openFT instance

openFT instances that are able to be administered by *remote administrators* during live operation.

admission profile

Way of defining the *FTAC* protection functions. Admission profiles define a *transfer admission* that has to be specified in *FT requests* instead of the *LOGON* or *Login authorization*. The admission profile defines the *access rights* for a user ID by restricting the use of parameters in *FT requests*.

admission profile, privileged

see *privileged admission profile*

admission set

In *FTAC*, the admission set for a particular user ID defines which FT functions the user ID may use and for which *partner systems*.

admission set, privileged

see *privileged admission set*

AES (Advanced Encryption Standard)

The current symmetrical encryption standard, established by NIST (National Institute of Standards and Technology), based on the Rijndael algorithm, developed at the University of Leuven (B). The openFT product family uses the AES method to encrypt the request description data and possibly also the file contents.

alphanumeric

Alphanumeric characters comprise alphabetic and numeric characters, i.e. the letters A-Z and the digits 0-9.

ANSI code

Standardized 8-bit character code for message exchange. The acronym stands for "American National Standards Institute".

API (Application Programming Interface)

An interface that is freely available to application programmers. It provides a set of interface mechanisms designed to support specific functionalities.

Application Entity Title (AET)

The Application Entity Title consists of Layer 7 addressing information of the *OSI Reference Model*. It is only significant for *FTAM partners*.

asynchronous request

Once the *FT request* has been submitted, it is processed independently of the user. The user can continue working once the system has confirmed acceptance of the request. (see also *synchronous request*).

audit

Fundamental function of a secure system; logging of operating sequences and preparation of the logged data.

authentication

Process used by openFT to check the unique identity of the request partner.

basic functions

Most important file transfer functions. Several basic functions are defined in the *admission set* which can be used by a login name. The six basic functions are:

- inbound receive
- inbound send
- inbound follow-up processing
- inbound file management
- outbound receive
- outbound send

central administration

Central administration in openFT incorporates the *remote administration* and *ADM traps* functions and requires the use of a *remote administration server*.

character repertoire

Character set of a file in the *virtual filestore*.
In the case of files transferred with *FTAM partners* it is possible to choose between: *GeneralString*, *GraphicString*, *IA5String* and *VisibleString*.

Character Separated Values (CSV)

This is a quasi-tabular output format that is very widely used in the PC environment in which the individual fields are separated by a separator (often a semicolon “;“). It permits the further processing of the output from the most important openFT commands using separate tools.

client

- Term derived from client/server architectures: the partner that makes use of the services provided by a *server*.
- Logical instance which submits requests to a *server.*

cluster

A number of computers connected over a fast network and which in many cases can be seen as a single computer externally. The objective of clustering is generally to increase the computing capacity or availability in comparison with a single computer.

Comma Separated Values

see *Character Separated Values.*

communication computer

Computer for constructing a *data communication system*.

communication controller

see *preprocessor*

compression

This means that several identical successive characters can be reduced to one character and the number of characters is added to this. This reduces transfer times.

computer network, open

see *open computer network*

concurrency control

Component of the FTAM file attribute *access control* (part of the *security group*) in the *virtual filestore* that controls concurrent access. openFT for BS2000 offers only passive and partial support for concurrency control. Note: “partial support” is a technical term taken from the FTAM environment that means that the parameter is interpreted correctly at the syntactic level but is not genuinely supported.

configuration user ID

Each openFT instance in BS2000 requires an ID, on which the variable files of this file are stored (for the default instance: $SYSFJAM).

connectivity

In general, the ability of systems and partners to communicate with one another. Sometimes refers simply to the communication possibilities between transport systems.

constraint set

Component of the *document type*.

contents type

File attribute in the *virtual filestore,* attribute of the *kernel group* that describes the file structure and the form of the file contents.

cross domain connection

Connection mode in which a TRANSDATA network is connected as an SNA domain to an SNA domain via a *gateway*.

DASD (Direct Access Storage Device)

Disk storage

data communication system

Sum of the hardware and software mechanisms which allow two or more communication partners to exchange data while adhering to specific rules.

data compression

Reducing the amount of data by means of compressed representation.

data encoding

Way in which an *FT system* represents characters internally.

Data Encryption Standard (DES)

International data encryption standard for improved security. The DES procedure is used in the FT products to encrypt the request description data and possibly the request data if connections are established to older versions of openFT that do not support *AES*.

data protection

– In the narrow sense as laid down by law, the task of protecting personal data against misuse during processing in order to prevent the disclosure or misappropriation of personal information.
– In the wider sense, the task of protecting data throughout the various stages of processing in order to prevent the disclosure or misappropriation of information relating to oneself or third parties.

data security

Technical and organizational task responsible for guaranteeing the security of data stores and data processing sequences, intended in particular to ensure that

– only authorized personnel can access the data,
– no undesired or unauthorized processing of the data is performed,
– the data is not tampered with during processing,
– the data is reproducible.

DHCP

Service in TCP/IP networks that automatically assigns IP addresses and TCP/IP parameters to clients on request.

directory

Directories are folders in the hierarchical file system of a Unix system (including POSIX) or a Windows system that can contain files and/or further directories. In BS2000 (DVS), PLAM libraries are interpreted as directories.

document type

Value of the file attribute *contents type* (attribute of the *kernel group*). Describes the type of file contents in the *virtual filestore*.

– *document type* for text files: FTAM-1
– *document type* for binary files: FTAM-3

dynamic partner

partner system that is either not entered in the *partner list* (*free dynamic partner*) or that is entered in the partner list with only address but without a name (*registered dynamic partner*).

emulation

Components that mimic the properties of another device.

entity

see *instance*

Explorer

A program from Microsoft that is supplied with Windows operating systems to facilitate navigation within the file system.

file attributes

A file’s properties, for example the size of the file, access rights to the file or the file’s record structure.

file directory / file catalog

File present in every *pubset* (in SM pubsets there is a file directory in every volume set). All a pubset’s files and job variables are entered in the corresponding *file directory*. Files on private disks and tapes can be entered in the file directory.
A catalog entry contains all a file’s or job variable’s attributes (protection attributes, location of the administered data etc.

file management

Possibility of managing files in the remote system. The following actions are possible:

- Create directories
- Display and modify directories
- Delete directories
- Display and modify file attributes
- Rename files
- Delete files.

file processing

The openFT “file processing” function makes it possible to send a receive request in which the output of a remote command or program is transferred instead of a remote file.

filestore, virtual

see *virtual filestore*

file transfer request

see *FT- request*

firewall processor

Processor which connects two networks. The possible access can be controlled precisely and also logged.

fixed-length record

A record in a file all of whose records possess the same, agreed length. It is not necessary to indicate this length within the file.

follow-up processing

FT function that initiates execution of user-specified commands or statements in the *local* and/or the *remote system* after an *FT request* has been completed. The user may define different follow-up processing, depending on the success or failure of FT request processing. See also *preprocessing* and *postprocessing*.

follow-up processing request

Statements contained within an *FT request* which perform *follow-up processing* after file transfer.

free dynamic partner

Partner system that is not entered in the partner list.

FT administrator

Person who administers the openFT product installed on a computer, i.e. who is responsible, among other things, for the entries in the *network description file* or the *partner list* as well as for controlling resources.

FT request

Request to an *FT system* to transfer a file from a *sending system* to a *receive system* and (optionally) start *follow-up processing requests*.

FT system

System for transferring files that consists of a computer and the software required for file transfer.

FT trace

Diagnostic function that logs FT operation.

FTAC (File Transfer Access Control)

Extended access control for file transfer and file management. In the case of BS2000 and z/OS, this is implemented by means of the product openFT-AC, for other operating systems it is a component of the openFT product, e.g. in openFT for Unix systems or openFT for Windows systems.

FTAC administrator

Administrator of the FTAC functions; should be identical to the person responsible for data security in the system.

FTAC logging function

Function which FTAC uses to log each access to the protected system via file transfer.

FTADM protocol

Protocol used for communication between two openFT instances in order to perform *remote administration* or transfer *ADM traps*.

FTAM file attributes

All systems which permit file transfer via FTAM protocols must make their files available to their partners using a standardized description (ISO 8571). To this end, the attributes of a file are mapped from the physical filestore to a *virtual filestore* and vice versa. This process distinguishes between three groups of file attributes:

- kernel group: describes the most important file attributes.
- storage group: contains the file’s storage attributes.
- security group: defines security attributes for file and system access control.

FTAM partner

Partner system that uses *FTAM protocols* for communication.

FTAM protocol (File Transfer, Access and Management)

Protocol for file transfer standardized by the “International Organization for Standardization” (ISO) (ISO 8571, FTAM).

FTP partner

Partner system that uses *FTAM protocols* for communication.

FTP protocol

Manufacturer-independent protocol for file transfer in TCP/IP networks.

functionality class

Class which places certain minimum security function demands on an IT system.
The functionality classes are defined in the “Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)”, (Criteria for the assessment of the security of Information Technology (IT) systems), version 1 of 11th January 1989, published by the Zentralstelle für Sicherheit in der Informationstechnik (Central Office for Security in Information technology) on behalf of the German government.

functional standard

Recommendation defining the conditions and the forms of application for specific ISO standards (equivalent term: *profile*). The transfer of unstructured files is defined in the European Prestandard CEN/CENELEC ENV 41 204; file management is defined in the European Prestandard CEN/CENELEC ENV 41205.

gateway

Generally understood to mean a computer that connects two or more networks and which does not function as a bridge. Variants: gateway at network level (= router or OSI relay), transport and application gateway.

gateway processor

Communication computer that links a computer network to another computer network. The mapping of the different protocols of the various computer networks takes place in gateway processors.

general string

Character repertoire for file files transferred to and from *FTAM partners*.

global privileges

All the privileges that can be assigned using the /SET-PRIVILEGE command including the security administrator privilege and the TSOS privilege. Global privileges and *system administrator privileges* are identical.

global request identification / global request ID / global request number

Request number that the *initiator* of an openFT or FTAM request transfers to the *responder*. This means that the global request ID in the responder is identical to the *request ID* in the initiator. The responder generates its own (local) request ID for the request. This means that information stored in both the initiator and the responder can be unambiguously assigned to a request. This is particularly important if the request has to be restarted.

global user administration

This comprises the administration of user IDs and user groups and covers resources and user rights, the creation, modification and deletion of user IDs and user groups

GraphicString

Character repertoire for files transferred to and from *FTAM partners*.

guard

A component of the GUARDS condition administration system. A guard unites conditions which are evaluated by the standard GUARDS condition administration system on request.

GUARDS (Generally Usable Access Control Administration System)

Object administration for *Guards*.

heterogeneous network

A network consisting of multiple subnetworks functioning on the basis of different technical principles.

homogeneous network

A network constructed on the basis of a single technical principle.

host

Formerly a large-scale data processing system which required a *front-end processor* in order to be able to communicate. Nowadays, the term used for BS2000 or z/OS systems.

IA5String

Character repertoire for files transferred to and from *FTAM partners.*

identification

Procedure making it possible to identify a person or object.

inbound file management

Request issued in a *remote system* for which directories or file attributes of the *local system* can be displayed, file attribute modified or local file deleted.

inbound follow-up processing

Request issued in a *remote system* with *follow-up processing* in the *local system*.

inbound receive

Request issued in the *remote system*, for which a file is received in the *local system*.

inbound request / inbound submission

Request issued in another system, i.e. for this request.

inbound send

Request issued in a *remote system* for which a file is sent from the *local system* to the remote system.

initiator

Here: *FT system* that submits an *FT request*.

instance / entity

A concept of OSI architecture: active element in a layer. Also see *openFT instance*.

instance ID

A network-wide, unique address of an openFT instance.

integrity

Unfalsified, correct data following the processing, transfer and storage phases.

interoperability

Capability of two *FT systems* to work together.

ISO/OSI reference model

The ISO/OSI Reference Model is a framework for the standardization of communications between open systems. (ISO=International Standards Organization).

job

Sequence of commands, statements and data.

job class

Job classes combine *jobs* which share certain properties and characteristics.

job transfer

Transfer of a file that constitutes a *job* in the *receive system* and is initiated as a job there.

joinfile / user catalog / user ID catalog

File that contains the *user attributes* of all the *user IDs* in a *pubset*.

kernel group

Group of file attributes of the *virtual filestore* that encompasses the kernel attributes of a file.

library

File with internal structure (members)

library member

Part of a library. A library member may in turn be subdivided into a number of records.

Local Area Network (LAN)

Originally a high-speed network with limited physical extension. Nowadays, any network, that uses CSMA/CD, Token Ring or FDDI irrespective of the range (see also *WAN Wide Area Network*).

local system

The *FT system* at which the user is working.

logging function

Function used by openFT to log all file transfer accesses to the protected system.

log record

Contains information about access checks performed by openFT (FTAC log record) or about a file transfer or remote administration request which is started when the access check was successful (FT log record or ADM log record).

Logical Unit (LU)

Interface between an application program and the SNA data communications network. The LU type describes the communications characteristics.

Login authorization

Transfer admission to a computer which (as a rule) consists of the login name and the password, and authorizes dialog operation, see also *LOGON authorization*.

LOGON authorization

Transfer admission authorizing access to a computer. The LOGON authorization (normally) consists of user ID, account number and password and authorizes the user to make use of interactive operation.

mainframe

Computer (consisting of one or more processors) which runs under the control of a universal operating system (e.g. BS2000 or z/OS).
Synonyms: BS2000 computer, host computer.

maximum-string-length

Specifies the maximum length of *strings* within a file in the *virtual FTAM filestore*.

named partner

partner system entered by its name in the *partner list*.

Network Control Program (NCP)

Operating system of the front-end-processor for SNA hosts.

NEA

Name of a network architecture.

network description file

File used up to openFT V9 that contains specifications concerning *remote systems* (*FT systems*).

Network Management Kernel

Component of the Network Management Platform; responsible for forwarding network management requests as well as for centralized tasks such as logging, authorization checks, request and application administration.

object

Passive element in a DP system that contains or receives data and which can be the object of an operation such as read, write or execute etc.
Examples: files, user IDs

offline logging

The log file can be changed during operation. Following this changeover, the previous log file is retained as an offline log file; new log records are written to a new log file. It is still possible to view the log records in an offline log file using the tools provided by openFT.

open computer network

Computer network in which communication is governed by the rules of ISO/OSI. Interoperation of different computers from various vendors is made possible by defined *protocols*.

openFT instance

Several openFT systems, so-called openFT instances, can be running simultaneously on an individual computer or on the HIPLEX cluster. Each instance has its own address (instance ID, virtual BCAM host) and is comprised of the loaded code of the openFT products (including add-on products if they are available) and of the variable files such as the network description file or partner list, logging files, key library, request queue, etc.

openFT partner

Partner system which is communicated with using *openFT protocols*.

openFT protocols

Standardized *protocols* for file transfer (SN77309, SN77312).

openFT-FTAM

Add-on product for openFT (for BS2000, Unix systems and Windows systems) that supports file transfer using FTAM protocols. FTAM stands for File Transfer, Access and Management (ISO 8571).

operating parameters

Parameters that control the *resources* (e.g. the permissible number of connections).

outbound request / outbound submission

Request issued in your own processor.

outbound receive

Request issued locally for which a file is received in the *local system*.

outbound send

Request issued locally for which a file is sent from the *local system*.

owner of an FT request

User ID in the *local system* or *remote system* under which the *FT request* is started (or submitted). The owner is always the ID under which the request is submitted, not the ID under which it is executed.

partner

see *partner system*

partner list

File containing specifications concerning *remote systems* (*FT systems*).

partner system

Here: *FT system* that carries out *FT requests* in cooperation with the *local system*.

password

Sequence of characters that a user must enter in order to access a user ID, file, job variable, network node or application. The user ID password serves for user *authentication*. It is used for access control. The file password is used to check access rights when users access a file (or job variable). It is used for file protection purposes.

permitted actions

File attribute in the *virtual filestore*; attribute of the *kernel group* that defines actions that are permitted in principle.

Personal Audit for Individual Accountability

Trace of individual system utilization. Identification can take the following forms:

- a user ID corresponds to a user, or
- a user may use only one operator terminal.

port number

Number that uniquely identifies a TCP/IP application or the end point of a TCP/IP connection within a processor.

POSIX (Portable Open System Interface)

Board and standards laid down by it for interfaces that can be ported to different system platforms.

postprocessing

openFT makes it possible to process the received data in the receiving system through a series of operating system commands. Postprocessing runs under the process control of openFT (in contrast to *follow-up processing*).

preprocessing

The preprocessing facility in openFT can be used to send a receive request in which the outputs of a remote command or program are transferred instead of a file. This makes it possible to query a database on a remote system, for example. Preprocessing also may be issued locally.

preprocessor / communication controller

A processor system connected upstream of the mainframe which performs special communication tasks in the network. Synonym: communication processor.

presentation

Entity that implements the presentation layer (layer 6) of the *ISO/OSI Reference Model* in an *FT system* that uses e.g. *FTAM protocols*.

presentation selector

Subaddress used to address a *presentation application*.

private key

Secret decryption key used by the recipient to decrypt a message that was encrypted using a *public key*. Used by a variety of encryption procedures including the *RSA procedure*.

privilege

- Global privilege within the system that authorizes a user to execute certain commands and call certain program interfaces (e.g. TSOS privilege).
- Set of user-specific attributes that are used by the access control system.

privileged admission profile

Admission profile that allows the user to exceed the *FTAC administrator's* presettings in the *admission set*. This must be approved by the *FTAC administrator* who is the only person able to privilege admission profiles.

privileged admission set

Admission set belonging to the *FTAC administrator*.

profile

In OSI, a profile is a standard which defines which protocols may be used for any given purpose and specifies the required values of parameters and options. Here: a set of commands assigned to a user ID. The permissibility of these commands is ensured by means of syntax files. See also *admission profile*, *privileged admission profile*.

protocol

Set of rules governing information exchange between peer partners in order to achieve a defined objective. This usually consists of a definition of the messages that are to be exchanged and the correct sequencing of messages including the handling of errors and other exceptions.

public key

Public encryption key defined by the receiver of a message, and made public or made known to the sender of the message. This allows the sender to encrypt messages to be sent to the receiver. Public keys are used by various encryption methods, including the *Rivest Shamir Adleman (RSA) procedure*. The public key must match the *private key* known only to the receiver.

public space

Named disk storage area which is available to a defined number of user IDs within the operating system. This storage area may be located on one or more Public Volume Sets (*pubsets*).

pubset / public volume set

Set of shared, named disk storage units which is defined by a catalog identification (catid). A distinction is made between *SF pubsets* and SM pubsets.

receive file

File in the *receive system* in which the data from the *send file* is stored.

receive system

System to which a file is sent. This may be the *local system* or the *remote system*.

record

Set of data that is treated as a single logical unit.

registered dynamic partner

Partner system that is entered in the partner list with only an address but no name.

relay

OSI term for an element in a layer that acts as an intermediary between two other partners and thus makes communications between these two partners possible.
In the narrow sense, on the network layer a relay is the functional equivalent of a *router*.

relay program

Program in a *gateway processor* that maps the different protocols onto one another.

remote administration

Administration of openFT instances from remote computers.

remote administration server

Central component required for *remote administration* and for *ADM traps*. A remote administration server runs on a Unix or Windows system running openFT as of V11.0. If it is used for *remote administration*, it contains all the configuration data required for this purpose.

remote administrator

Role configured on the *remote administration server* and which grants permission to execute certain administration functions on certain openFT instances.

remote system

see *partner system*

request

see *FT request,*

request queue

File containing *asynchronous requests* and their processing statuses.

request identification / request ID / request number

The (serial) number assigned to the request by the local system. In some commands, users are able to identify the request on the basis of this number. Here: Number assigned by the local system that identifies an *FT request.*

request management

FT function responsible for managing *FT requests*; it ensures request processing from the submission of a request until its complete processing or termination.

request number

see *request identification*

request storage

FT function responsible for storing *FT requests* until they have been fully processed or terminated.

resources

Hardware and software components needed by the *FT system* to execute an *FT request* (*tasks*, connections, lines). These resources are controlled by the *operating parameters*.

responder

Here: *FT system* addressed by the *initiator*.

restart

Automatic continuation of an *FT request* following an interruption.

restart point

Point up to which the data of the *send file* has been stored in the *receive file* when a file transfer is interrupted and at which the transfer of data is resumed following a *restart*.

result list

List with information on a completed file transfer. This is supplied to the user in the *local system* and contains information on his or her *FT requests*.

RFC (Request for Comments)

Procedure used on the Internet for commenting on proposed standards, definitions or reports. Also used to designate a document approved in this way.

RFC1006

Supplementary protocol for the implementation of ISO transport services (transport class 0) using TCP/IP.

Rivest-Shamir-Adleman-procedure (RSA procedure)

Encryption procedure named after its inventors that operates with a key pair consisting of a *public key* and a *private key*. Used by the openFT product family in order to reliably check the identity of the partner system and to transmit the AES key to the partner system for encrypting the file contents.

router

Network element that is located between networks and guides message flows through the networks while simultaneously performing route selection, addressing and other functions. Operates on layer 3 of the OSI model.

RPC (Remote Procedure Call)

Cross-network server procedure call issued by client.

security attributes

An object's security attributes specify how and in what ways the object may be accessed.

Secure FTP

Method by which a connection is tunneled using the *FTP protocol*, thus allowing secure connections with encryption and *authentication*.

security group

Group of file attributes in the *virtual filestore*, encompassing the security attributes of a file.

security level

When FTAC is used, the security level indicates the required level of protection against a *partner system*.

send file

File in the *sending system* from which data is transferred to the *receive file*.

sending system

Here: *FT system* that sends a file. This may be the *local system* or the *remote system*.

server

Logical entity or application component which executes a client's requests and assures the (coordinated) usage of all the generally available services (File, Print, data base, Communication, etc.). May itself be the client of another server.

service

- As used in the OSI architecture: a service is the set of functions that a service provider makes available at a service access point.
- As used in the client/server architecture: a set of functions that a server makes available to its clients.
- Term used in Unix and Windows systems: A program, routine or process used to perform a particular system function to support other programs, in particular on a low level (hardware-related).

service class

Parameter used by *FTAM partners* to negotiate the functions to be used.

session

- In OSI, the term used for a layer 5 connection.
- In SNA, a general term for a connection between communication partners (applications, devices or users).

session selector

Subaddress used to address a *session* application.

SF pubset (Single Feature Pubset)

One or more disks whose key properties (disk format, allocation unit) match and which are used to store files and JVs under a shared catalog ID.

SNA network

Data communication system that implements the Systems Network Architecture (SNA) of IBM.

SNMP (Simple Network Management Protocol)

Protocol for TCP/IP networks defined by the Internet Engineering Task Force (IETF) for the transfer of management information.

standard admission set

This standard admission set applies by default to all users for whom there is no dedicated admission set. These default settings may be restricted further by the user for his or her own admission set.

Standard Access Control

Consists of the ACCESS and USER-ACCESS rights that are defined in the CREATE-FILE or MODIFY-FILE-ATTRIBUTES commands.

standard instance

The first openFT-instance that is loaded after /START-SUBSYSTEM FT. By default all openFT commands refer to this instance, if no other instance was specified with the command /SET-FT-INSTANCE. It is displayed as the first instance in the output of /SHOW-FT-INSTANCE INSTANCES=*ALL.

storage group

File attribute in the *virtual filestore*, encompasses the storage attributes of a file.

string

Character string

string significance

Describes the format of *strings* in files to be transferred using *FTAM protocols*.

subject

Active element in a data processing system from which an operation such as read, write, execute etc. can be initiated, that can cause a flow of information or can change the system status, e.g. ID, program, program component.

subsystem

Part of a system which processes a self-contained group of functions.

synchronous request

The user task that submitted the *FT request* waits for transfer to terminate. The user cannot continue working (see also *asynchronous request*).

SYSFILE environment

System files; the SYSFILE environment designates the totality of the system files assigned to a request.

system

see *FT- system*

system, local

see *local system*

system, remote

see *remote system*

system administration

- Structural unit in the computer center
- Group of individuals who employ user IDs that are associated with global privileges.

system administrator command

Command which cannot be submitted by any user ID but only by user IDs which possess the corresponding global privileges or by the TSOS user ID.

system administrator privileges

see *global privileges*

system files

The system input/output files assigned to a request. Users can only access system files indirectly by means of the SYSFILE command. System files provide data and resources that are required for the functions of the control program. System files and their primary allocations:

- SYSOUT: output of system messages to terminals
- SYSLST: output of compilation logs etc.via printer (automatic SPOOLOUT)
- SYSLSTnn: as SYSLST; 1 ≤ nn ≤ 99; each of the max.99 system files must be assigned to a cataloged file
- SYSOPT: output file as SYSLST
- SYSCMD: used to submit commands to the control program
- SYSDTA: used to enter data or statements

system resources

Resources in a computer system that can be requested or released by a *job* or a *task*.

task

Entity responsible for processes. In BS2000 tasks are used, among other things, to process user jobs (e.g. batch jobs, interactive jobs), see *job*.

TCP/IP (Transmission Control Protocol / Internet Protocol)

Widely used data transmission protocol (corresponds approximately to layers 3 and 4 of the *ISO/OSI reference model*, i.e. network and transport layers); originally developed for the ARPANET (computer network of the US Ministry of Defense) it has now become a de-facto standard.

Top Secret

Program authored by the company Computer Associates for data and system access control.

transfer admission

Authorization for file transfer and file management when using FTAC. The transfer admissions is then used in place of the *LOGON or LOGIN authorization*.

transfer unit

In an FTAM environment, the smallest data unit for transporting file contents. For *FTAM-1* and *FTAM-3* these are *strings*. A transfer unit can, but need not, correspond to one file record.

Transmission Control Protocol / Internet Protocol

see *TCP/IP*

TranSON

TranSON is a software product that permits secure access to a server. The use of TranSON is transparent to the application. The connection to the remote partner goes from the workstation through a client proxy and server proxy to the remote partner. The client proxy is located on the workstation, and the server proxy is located on the remote partner. The data transferred between the client proxy and the server proxy is encrypted.

transport connection

Logical connection between two users of the transport system (terminals or applications).

transport layer

Layer 4 of the *ISO/OSI reference model* on which the data transport protocols are handled.

transport protocol

Protocol used on the *transport layer*

transport selector (T-selector)

Subaddress used to address an ISO-8072 application in the *transport layer*.

transport system

- The part of a system or architecture that performs approximately the functions of the four lower OSI layers, i.e. the transport of messages between the two partners in a communication connection.
- Sum of the hardware and software mechanisms that allow data to be transported in computer networks.

TSN (Task Sequence Number)

Identification of a BS2000 process (*task*).

Unicode

The universal character encoding, maintained by the Unicode Consortium. This encoding standard provides the basis for processing, storage and interchange of text data in any language in all modern software and information technology protocols. The Unicode Standard defines three Unicode encoding forms: UTF-8, UTF-16 and UTF-32.

universal-class-number

Parameter of the *document-type* that defines the *character-repertoire* of a file to be transferred.

UNIX®

Registered trademark of the Open Group for a widespread multiuser operating system. A system may only bear the name UNIX if it has been certified by the Open Group.

Unix system

Commonly used designation for an operating system that implements functions typical of UNIX® and provides corresponding interfaces. POSIX and Linux are also regarded as Unix systems.

user

Represented by a *user ID*. The term “user” is a synonym for individuals, applications, procedures etc. which can obtain access to the operating system via a user ID.

user administration

see *global user administration*

user attributes

All the characteristics of the *user ID* that are stored in the *joinfile*.

user command

Command that can be issued under any *user identification* in system mode (/) or in program mode by means of a CMD macro.

user identification / user ID

A name with a maximum length of eight characters which is entered in the joinfile. The user ID identifies the user when accessing the system. All files and job variables are set up under a user ID. The names of the files and job variables are stored in the *file catalog* together with the user ID.

user privileges

All the attributes that represent rights that are assigned to a *user identification* and are stored in the *joinfile*.

variable length record

A record in a file all of whose records may be of different lengths. The record length must either be specified in a record length field at the start of the record or must be implicitly distinguishable from the next record through the use of a separator (e.g. Carriage Return - Line Feed).

virtual filestore

The FTAM virtual filestore is used by *FT systems* acting as *responders* to make their files available to their *partner systems*. The way a file is represented in the virtual filestore is defined in the FTAM standard, see *file attributes*.

VisibleString

Character repertoire for files transferred to and from *FTAM partners*.

volume set

Component of an SM pubset. A volume set is a set of disks whose key properties (disk format, allocation unit) match.
The name of the volume set is administered in a directory of the SM pubset. However, the data on a volume in the volume set is addressed via the SM pubset ID.

WAN (Wide Area Network)

A public or private network that can span large distances but which runs relatively slowly and with higher error rates when compared to a *LAN*. Nowadays, these definitions have only limited validity. Example: in ATM networks.

Abbreviations

ACSE	Association Control Service Element
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
API/CS	Application Programming Interface/Communication System
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASECO	Advanced SEcurity COntrol (BS2000, SINIX)
ASN	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
BCAM	Basic Communication Access Method
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAE	Common Application Environment
CCP	Communication Control Program
CCS	Coded Character Set
CCSN	Coded Character Set Name
CDDI	Copper Distributed Data Interface
CEN	Comité Européen de Coordination des Normes
CENELEC	Comité Européen de Normalisation Electrotechnique
CICS	Customer Information Control System (IBM)
CMX	Communication Manager SINIX
COM	Communication Port (asynchronous)
CPX	Compact Packet Exchange
DAS	Data Access Service
DAP	Directory Access Protocol

DBA	Data Base Access Service
DCAM	Data Communication Access Method
DCE	Data Communication Equipment
DCE	Distributed Computing Environment (OSF)
DCM	Data Communication Method
DDV	Datendirektverbindung (früher HfD)
DES	Data Encryption Standard (NBS)
DFR	Document File Retrieval
DFS	Distributed File System (DCE)
DIN	Deutsches Institut für Normung
DME	Distributed Management Environment
DMS	Data Management Service
DNS	Domain Name Service
DOS	Disk Operating System
DSA	Directory System Agent
DSC	Data Stream Compatibility
DSM	Distributed Systems Management
DSP	Directory System Protocol
DSS	Datensichtstation
DSSM	Dynamic Subsystem Management
DTE	Data Termination Equipment
DTS	Distributed Time Service
DVA	Datenverarbeitungsanlage
DVS	Datenverwaltungssystem
EBCDIC	Extended Binary-Coded Decimal Interchange Code
EMDS	Emulation Datensichtstation
EN	European Norm
ENV	Europäischer Normen-Vorschlag
EPHOS	European Procurement Handbook for Open Systems
ERMS	Entity Relationship Management System
ES	End System
ETSI	European Telecommunication Standards Institute
EWOS	European Workshop for Open Systems

FADU	File Access Data Unit
FDDI	Fiber Distributed Data Interface
FEP	Front End Processor
FJAM	File Job Access Method
FT	File Transfer
FTAC	File Transfer Access Control
FTAM	File Transfer, Access and Management (ISO 8571)
FTP	File Transfer Protocol
GOSIP	Government OSI Profile
HDLC	High Level Data Link Control (ISO 7776)
HNC	Highspeed Net Connect
HPFS	High Performance File System
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
ICC	Intelligent Communication Controller
ICMP	Internet Control Message Protokoll
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IGMP	Internet Group Management Protocol
IMS	Information Management System (IBM)
IP	Internet Protocol
ISAM	Index Sequential Access Method
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria (Europe, White Book)
ITU	International Telecommunication Union
JCL	Job Control Language
LAN	Local Area Network
LMS	Library Maintenance System
LU	Logical Unit
MAC	Medium Access Control
MAN	Metropolitan Area Network

MCR	Magnetic Card Reader
MIB	Management Information Base
MLC	Modular LAN Connect
MSV	Mittelschnelles Synchron Verfahren
MVS	Multiple Virtual System
NCP	Network Control Program (SNA)
NCS	Network Control System
NDMS	Network Data Management System
NEA	(Name der TRANSDATA-Architektur von Siemens)
NFS	Network File System
NTP	Network Time Protocol
ODI	Open Data Link Interface
ODI	Open Device Interface
ODL	Object Description Language
OSI	Open Systems Interconnection
OSS	OSI Session Service
PAM	Primary Access Method
PC	Personal Computer
PDN	Programmsystem für Datenübertragung und Netzsteuerung
PDU	Protocol Data Unit
PEM	Privacy Enhanced Mail
PICS	Protocol Implementation Conformance Statement
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PLAM	Primary Library Access Method
POP	Post Office Protocol
POSIX	Portable Operating System Interface for Open Systems
PSDN	Packet Switched Data Network
PU	Physical Unit
RFC	Request for Comments
RFC1006	Request for Comments 1006
RJE	Remote Job Entry
RPC	Remote Procedure Call

RTS	Reliable Transfer Service
SAM	Sequential Access Method
SAP	Server Advertising Protocol (NetWare)
SAP	Service Access Point (OSI)
SBS	Siemens Business Services
SCM	Software Configuration Management
SDF	System Dialog Facility
SDLC	Synchronous Data Link Control
SESAM	System zur Elektronischen Speicherung Alphanumerischer Merkmale
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TELNET	Telecommunications Network Protocol
TFTP	Trivial File Transfer Protocol
TID	Transport Identification
TS	Transport System
UDP	User Datagram Protocol
UDS	Universelles Datenbanksystem
URL	Uniform Resource Locator
UTM	Universal Transaction Monitor
VDE	Verband deutscher Elektrotechniker
WAN	Wide Area Network
WS	Workstation
XDR	External Data Representation
XDS	API to Directory Service

Related publications

You will find the manuals on the internet at *http://manuals.ts.fujitsu.com*. You can order manuals which are also available in printed form at *http://manualshop.ts.fujitsu.com*.

openFT V12.0 for BS2000/OSD
Managed File Transfer in the Open World
User Guide

openFT V12.0 for BS2000/OSD
Program Interfaces
Programmer Reference Guide

openFT V12.0 for Unix Systems
Managed File Transfer in the Open World
User Guide

openFT V12.0 for Unix Systems
Installation and Administration
System Administrator Guide

openFT V12.0 for Windows Systems
Managed File Transfer in the Open World
User Guide

openFT V12.0 for Windows Systems
Installation and Administration
System Administrator Guide

openFT V12.0 for Unix Systems and Windows Systems
Program Interface
User Guide

openFT V12.0 for Unix Systems and Windows Systems
openFT-Script Interface
User Guide)

openFT V12.0 for z/OS
Managed File Transfer in the Open World
User Guide

openFT V12.0 for z/OS
Installation and Administration
System Administrator Guide

openNet Server (BS2000/OSD)
BCAM
User Guide

SNMP Management
SNMP Management for BS2000/OSD
User Guide

BS2000/OSD-BC
Commands (multiple volumes)
User Guide

BS2000/OSD
Executive Macros
User Guide

IMON (BS2000/OSD)
Installation Monitor
User Guide

BS2000/OSD-BC
Introductory Guide to DMS
User Guide

BS2000/OSD-BC
Subsystem Management (DSSM/SSCM)
User Guide

BS2000/OSD-BC
System Installation
User Guide

BS2000/OSD-BC
Introductory Guide to Systems Support
User Guide

JV (BS2000/OSD)
Job Variables
User Guide

SECOS (BS2000/OSD
Security Control System
User Guide

XHCS (BS2000/OSD)
8-Bit Code and Unicode Support in BS2000/OSD
User Guide

HIPLEX (BS2000/OSD)
High availability of applications in BS2000/OSD
Product manual

Index