

***openFT-AC* (BS2000/OSD) Version 10.0**

Issue March 2007

Extended Access Protection for *openFT*

Pages 3

openFT-AC for BS2000/OSD is a software product that can be used in BS2000/OSD with *openFT*, FTAM, and FTP partners. In addition to the protection functions provided by BS2000/OSD and *openFT*, *openFT-AC* offers extended access protection and hence even greater security for file transfers. *openFT-AC* extends *openFT* by the addition of the FTAC (File Transfer Access Control) component, which offers the following functions and features:

- The FTAC administrator is able to precisely delimit and define the file transfer rights of both the local users and the FT partner systems.
- With FTAC, access authorization for file transfer is decoupled from the LOGON authorization, i.e. the FTAC transfer admission does not permit access to interactive processing.
- The definition of access rights remains straightforward even in large networks.
- The logging file contains information on all the access checks that have been performed, enabling them to be audited if necessary.
- The protection mechanisms are easy to use for both the FTAC administrator and the user.
- Flexible graduation of the access and follow-up processing rights is provided.
- Follow-up processing commands can be specified taking variables into account. Users in remote systems are therefore independent of the BS2000 syntax and inbound follow-up processing is also possible for FTAM partners.
- Access rights can be restricted to a predefined task for each partner individually, so that certain tasks are no longer allowed (e.g. follow-up processing).
- Access rights can be allocated both for *openFT* partners (the file transfer protocol from Fujitsu Siemens Computers) and for FTAM partners (the file transfer protocol standardized by ISO).
- Access authorization once granted can be modified or cancelled later.

FTAC combines straightforwardness with flexibility in two ways. Firstly, the structuring of the partner systems into security levels and of the functions into basic functions provides a simple means of defining interdependencies. Secondly, a two-stage mechanism is provided for defining the access rights. The definition of access rights by way of user-specific authorization records is used as a coarse method of control. Fine control of the access rights is possible with the aid of authorization profiles.

Security levels

Each partner system is assigned to a security zone when it is entered in the partner list. Each security zone is assigned a numerical value between 1 and 100, this being the security level. The security level reflects the degree of protection required with respect to a partner system (1 = level with the smallest security requirement, 100 = level with the greatest security requirement). The system of security levels is hierarchical, i.e. once an access authorization has been assigned for a security level, it applies for all lower security levels.

Basic functions

There are six basic functions:

- outbound send
local request in response to which a file is transmitted from the local system
- outbound receive
local request in response to which a file is received in the local system
- inbound send
remote request in response to which a file is transmitted from the local system
- inbound receive
remote request in response to which a file is received in the local system
- inbound follow-up processing
remote request with follow-up processing in the local system
- inbound file management
remote request to read or modify file attributes or file directories in the local system

Authorization record

For every user there is an authorization record which contains information indicating the security level up to which a basic function can be used. The authorization records are specified by the FTAC administrator. Users can restrict the limit values defining their protection requirements. In addition, the FTAC administrator can define limit values for a standard authorization record. This applies for all users for whom no individual definition has been made. The standard authorization record has the following benefits for the FTAC administrator:

- There is no need to register all users
- It provides a simple way of setting values for the majority of users

Authorization profile

The authorization profile is a user-defined access authorization. It defines which access rights are associated with this access authorization. Access rights are defined by permitting, restricting or forbidding the use of request parameters, e.g.

- specifying the transfer direction
- restricting access to a specific file or to files with a specific prefix
- permitting exactly one precisely defined follow-up processing or only follow-up processing commands with a specific prefix and/or suffix
- permitting exactly one precisely defined pre- or post-processing or only pre- or post-processing commands with a specific prefix

An authorization profile's requests are subject to the restrictions of the user authorization record. Users may only cancel the limit values they have defined themselves; they may not go beyond those defined by the FTAC administrator. There are also privileged authorization profiles for special cases. These can only be specified by the FTAC

administrator, who may exceed limit values he himself has set.

Import/export of authorization records and profiles

The FTAC administrator can swap out and save authorization rights and profiles of specific users.

Logging file

The logging file contains information on every access check performed with a remark indicating whether an FT request was accepted or, if it was not, the reason why it was rejected. The logging file also records who initiated the request and which file was to be transferred. The FTAC administrator has access to the entire logging data for all users, while users have only selective access to the requests relating to their own user ID. In conjunction with the FT log of *openFT BS2000/OSD*, which records file transfer execution, a complete overview is obtained.

User interface

A command interface, a graphical interface and a program interface are offered for administering (creating, modifying, displaying and deleting) the authorization rights and profiles. *openFT-AC* for BS2000/OSD can be used/administered from a Windows workstation via a graphical interface.

Changes since the preceding version V9.0

- For */CRE-FT-PRO* the default INITIATOR is changed from *REM to (*LOC,*REM).
- The length values for FILE-NAME and PARTNER has been changed.
- There is a Unix compatible Command Line Interface under Posix available.
- *openFT-AC* can be handled using the comfortable *openFT-Explorer* of *openFT V10* for Windows and Unix systems resp. (remote administration).

Technical Data	
Technical requirements for hardware	BS2000/OSD server. – Speicherbedarf (statisch): 246 KB
Technical requirements for software	<i>openFT-AC</i> for BS2000/OSD: – <i>openFT</i> V10.0 für BS2000/OSD – BS2000/OSD-BC as of V5.0 – openNet Server as of V3.0 – SDF as of V4.0 – POSIX-BC is a prerequisite for the support of POSIX files Graphical administration interface: – Windows 2003 or Windows XP – DOORS emulation or MT9750 as of V4.0 – DESK2000 as of V4.0 – <i>openFT-AC</i> for BS2000/OSD as of <i>openFT-AC</i> version 7.0
User interface	English und German, others on request.
Installation	By the customer on the basis of the release notice
Documentation	Manuals (English and German) for users and system administrators, in printed form via http://fsc-manualshop.com/ or as PDF files; also available on the Internet via http://www.fujitsu-siemens.com/openft
Demands on the user	BS2000 knowledge and if necessary knowledge of the partner system
Training	Courses are held in the Technical Training Academy von Fujitsu Siemens Computers under the currently valid conditions. For further information see http://training.fsc-mediaserver.com/elearningmedia/tectrac/
Conditions	This software product is supplied to the customer under the conditions for the use of software products against instalments or a single payment
Warranty	Class: A Delivery format: Machine language
Ordering and delivery	This software product may be obtained from your local Fujitsu Siemens Computers regional office