



TIBCO® Managed File Transfer Platform Server for z/OS

Security Guide

*Version 8.1.0
August 2021*



Contents

Contents	2
Introduction	3
Security Features	4
Authentication and Authorization	4
Password Management	5
File Transfer Modes	7
Hardware Compression and Encryption	8
Miscellaneous Security Features	8
Security Tasks	10
Preinstallation	10
Surrogate Checking	11
Installation and Configuration	12
Global Parameters	12
Node Parameters	15
Execution of File Transfers	16
Transfer Process Parameters	16
TIBCO Documentation and Support Services	18
Legal and Third-Party Notices	20

Introduction

TIBCO® Managed File Transfer Platform Server for z/OS is a peer-to-peer file transfer server that typically executes in the internal network, although it can also be used to transfer data over the internet. It is meant for very high transfer volume so it is efficient and fast.

This document describes guidelines to ensure security within TIBCO Managed File Transfer (MFT) Platform Server for z/OS. It provides security-related guidance and recommendations for installation, configuration, and execution of file transfers.

Security Features

TIBCO MFT Platform Server for z/OS provides many features that enhance security. These features are discussed in more detail later in the following sections:

- [Authentication and Authorization](#)
- [Password Management](#)
- [File Transfer Modes](#)
- [Hardware Compression and Encryption](#)
- [Miscellaneous Security Features](#)

Authentication and Authorization

All file transfers are executed under the authority of the user that executes the transfer:

- Initiator Transfers
- Responder Transfers

Initiator Transfers

For transfers initiated by TIBCO MFT Platform Server for z/OS:

- The user ID of the user initiating the transfer
 - If a local user/password was defined, the authorization of this user
 - If a surrogate local user was defined, the authorization of this user

For transfers initiated by TIBCO MFT Command Center:

- The user ID/password sent by Command Center

Responder Transfers

For transfers initiated by a responder:

- The user ID/password sent by the Platform Server client. When responder profiles are

used, the transfer is run under the authorization of the local user associated with the responder profile.

For TLS and TLS Tunnel requests, the user associated with the certificate. For information on certificate authentication, see the "SSL Authorization File" section in *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide* and the "SSL Authentication" section in *TIBCO® Managed File Transfer Platform Server for z/OS User's Guide*.

For more information on passwords and authentication, see the "Password Management" section of this document.

Password Management

TIBCO MFT Platform Server for z/OS supports the following two types of credentials:

1. User Profiles
2. Responder Profiles

For more information on user profiles and responder profiles, see the "User Profiles" section in the *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*.

User Profiles

User profiles allow a user or an administrator to define credentials when initiating transfers to a target node. Here is how user profiles work:

- User profiles are used when the remote user is set to *PROFILE and the remote password is not defined.
- Platform Server matches the user submitting the transfer and the target node defined for the transfer against user profile definitions created through the FUSPROF utility.
- When a match is found, these credentials are saved in the transfer and are sent to the remote system.

Advantages of Using User Profiles

- Passwords do not need to be included in the command line or in template files.
- The user initiating the transfers does not need to know the passwords of the remote

system.

i Note: When you want to use "User Profiles", set the remote user (RUSER) to *PROFILE. Example: RUSER=*PROFILE

Responder Profiles

Responder profiles are used when remote Platform Server clients initiate transfers to Platform Server for z/OS. Responder profiles match the credentials sent by the client against predefined credentials for that server. Here is how user profiles work.

- When a request is received, Platform Server matches the incoming IP address against the node definition table.
- Platform Server compares the node name of the incoming request and the user ID/password credentials contained in the request against the responder profiles created through the FUSPROF utility.
- When a match is found, the transfer is run under the rights of the local user associated with the responder profile.

Advantages of Using Responder Profiles

- The credentials used to connect to Platform Server for z/OS cannot log on to the z/OS system.
- You can reduce the number of RACF definitions required.

Responder profiles can be used for the following requests:

- File transfers initiated by Platform Server clients
- Command Center Collector and Audit Poll requests
- Command Center Node and Profile/RProfile requests
- Command Center Execute Platform Transfer requests

i Note: Platform Server user profiles and responder profiles can both be used on the same transfer.

Responder Profile Password Rules

You can define password complexity rules for responder profiles. For details, see "Responder Profile Password Rules" in the Global Configuration section.

File Transfer Modes

TIBCO MFT Platform Server for z/OS supports the following modes of operation for incoming and outgoing Platform Server requests. It is for both file transfer requests and administrative requests such as audit collection, server status, and node and profile updates.

- **Clear text mode.** The password is encrypted using a proprietary encryption algorithm but the data is not encrypted.
- **AES 256 encryption.** The password and data are encrypted using AES256. The asymmetric encryption key is generated through an algorithm on both the Client and Server. File Transfer Data is encrypted using the symmetric AES256 key.
- **SSL (or TLS) mode.** MFT establishes an SSL connection with the partner server. A symmetric AES 256 encryption key is exchanged through the secure TLS connection. MFT uses this AES256 encryption key to encrypt and decrypt all data. MFT also adds a message digest and sequence number to each record to prevent man in the middle attacks.
- **Tunnel mode.** All data is sent over a negotiated TLS connection. Each transfer creates a new TLS connection. The TLS Protocols and Ciphers can be configured in the Global section of the config.txt file.

Tunnel mode is the most secure option and is strongly suggested when communicating to partners over the internet. Tunnel mode requires TIBCO MFT Internet Server V8.2 and TIBCO MFT Platform Server V8.0 or higher.

When running in TLS/SSL or tunnel modes, Global parameters allow you to select the ciphers and TLS protocols(TLSv1, TLSv1.1, TLSv1.2).

Adding ZLIB compression adds an additional level of complexity to the encrypted data and makes it more difficult to decrypt the data.

SSLAUTH Configuration File

When using SSL/TLS or tunnel modes, additional validation can be performed. The SSLAUTH configuration is described in the "SSL Authorization Parameters" section of the *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*. This

file allows you to compare fields in the certificate DN (Distinguished Name) against predefined parameters in the SSLAUTH file. If a match is not made, the request is terminated with an error.

Hardware Compression and Encryption

If you have the necessary hardware, TIBCO MFT Platform Server for z/OS can use hardware instructions to encrypt and compress data. The CPU cycles required to encrypt and compress data are greatly reduced. Since CPU is reduced, you can encrypt and compress more data without worrying about consuming too many z/OS resources.

Miscellaneous Security Features

TIBCO MFT Platform Server for z/OS includes two features, documented in the *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*, that can limit access to z/OS files: CFACCESS and CFALIAS. Both of these features are supported for responder transfers only.

CFACCESS

MFT Platform Server Access Control gives the administrator the ability to control file transfer capabilities for users and nodes. The administrator can restrict the following transfer functions:

- Send a file
- Receive a file
- Submit a job into the internal reader
- Execute a command
- The High Level Qualifier (HLQ) for a file SEND
- The High Level Qualifier (HLQ) for a file RECEIVE

Additionally, the administrator can restrict the following Post Processing Actions (PPA):

- Execute a command
- Submit a job into the internal reader
- Submit the DSN for JCL into the internal reader

CFALIAS

MFT Platform Server File Alias Control gives the administrator the ability to provide an alias for a file based on the information about the initiator. In other words, you can tell the user to define the file name as DOG, and TIBCO MFT Platform Server CFALIAS changes that file name to an actual file name. You can define the following criteria:

- A USER
- A NODE or IP Address
- A combination of USER and NODE/IP Address

Additional criteria can be used to allow a user to supply aliases on a file:

- Send or Receive
- File name (as it exists on the mainframe)
- Alias file name (as entered by the user)

Security Tasks

It is a good practice to perform security-related tasks mentioned in the following sections:

- [Preinstallation](#)
- [Installation and Configuration](#)
- [Execution of File Transfers](#)

Preinstallation

Prior to installing TIBCO MFT Platform Server for z/OS, you must make the necessary RACF definitions for the Platform Server Started task. Prior to the installation, a user ID must be created for the Platform Server started task. This information is described in detail in the *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*.

Defining the Start Task User ID

There are 2 ways to define the start task user ID:

TRUSTED(Yes): If the value is Yes, the Platform Server started task has very high rights to datasets on the z/OS system.

TRUSTED(No): If the value is No, the Platform Server started task has limited rights to datasets on the z/OS system. You must define the MFT Platform Server user with the rights to access any datasets required by the Platform Server started task and the right to update password (if users are allowed to change their password through Platform Server).

When TRUSTED(No) is defined, you must set the following Global fields:

Field	Description
DNI_USERID	Defines the RACF user that will be used when using the DNI Feature. DNI scans for z/OS files matching filter criteria and transfers the files to a remote Platform Server. The DNI Scan is performed under the authorization of the Started

Field	Description
	Task user when this parameter is not defined. When this parameter is defined, the DNI Scan is performed under the authorization of the DNI_USERID. If a DNI transfer is performed, the transfer is executed under the authorization of the DNI_USERID.
SAPI_USERID	Defines the RACF user that will be used when using the SAPI (Sysout API) feature. The SAPI interface scans the JES queue for SYSOUT files matching filter criteria and transfers the SYSOUT data to a remote Platform Server. The SAPI scan is performed under the authorization of the Started Task user when this parameter is not defined. When this parameter is defined, the SAPI Scan is performed under the authorization of the SAPI_USERID. If a SAPI transfer is performed, the transfer is executed under the authorization of the SAPI_USERID.

Surrogate Checking

By default, TIBCO MFT Platform Server for z/OS runs transfers under the user ID of the user that initiated the transfer. If USERA wants to execute the transfer under the authorization of USERB, USERA can use one of the two choices provided:

1. Enter the local user ID and password of USERB when initiating the transfer.
2. Define a surrogate class that gives USERA the right to initiate transfers as USERB without specifying the password for USERB.



Note: Surrogate checking only applies to transfers initiated by TIBCO MFT Platform Server for z/OS. Surrogate checking is not performed when a Platform Server partner initiates a transfer to TIBCO MFT Platform Server for z/OS.

For additional RACF definitions, see the [Installation and Configuration](#) section.

Installation and Configuration

When installing or after you have installed TIBCO MFT Platform Server for z/OS, you must configure security-related parameters mentioned in the following sections based on your requirements:

- [Global Parameters](#)
- [Node Parameters](#)

Global Parameters

There are a variety of Global parameters that affect security mentioned in the following sections. For a detailed description of these parameters, see the "GLOBAL Startup Parameters" in *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*.

Security Parameters

Parameter	Description
ENFORCE_SECURITY_POLICY	<p>Defines the security policy for the Platform Server started task. You can configure the following values:</p> <p>NO: No security policy is defined.</p> <p>FIPS140: STC is FIPS140 compliant.</p> <p>TLSFIPS: TLS and Tunnel connections use FIPS compliant ciphers.</p> <p>HIPAA: HIPAA rules requiring encryption are followed.</p>
TLSCIPHERS	<p>Allows you to define ciphers used for TLS/SSL and Tunnel connections.</p>
TLSENABLEDPROTOCOL	<p>Defines the TLS protocols used (TLSv1, TLSv1.1, TLSv1.2).</p> <p>Responder Profile Password Rules:</p> <p>These parameters define the rules used when responder profiles are created. These rules apply to responder passwords created by the FUSPROF utility or through Command Center.</p>

Responder Profile Password Rule Parameters

These parameters define the rules used when responder profiles are created. These rules apply to responder passwords created by the FUSPROF utility or through Command Center.

- RPROFILE_PASSWORD_VALIDATION
- RPROFILE_MIN_LENGTH
- RPROFILE_MIN_UNIQUE
- RPROFILE_MIN_NUMBER
- RPROFILE_MIN_SPECIAL
- RPROFILE_MIN_LETTERS
- RPROFILE_REQUIRE_UPPER_LOWER

Communication Parameters

These parameters allow you to set the Adapter IP address that Platform Server uses when establishing TCP connections. You can set different Adapter IP address parameters for IPv4 and IPv6 and for Listen(Responder) and Connect(Initiator).

- TCPLISTEN_ADAPTER_IPADDR
- TCPLISTEN_ADAPTER_IPADDR_IPV6
- TCPCONNECT_ADAPTER_IPADDR
- TCPCONNECT_ADAPTER_IPADDR_IPV6

RACF Facility Class Checking Parameters

Parameter	Description
BOSSID	Defines users that can create profile and responder profile definitions.
CCC_BROWSE_FACILITY	Defines users that can perform audit inquiry via Command Center.
CCC_ALTER_FACILITY	Defines users that can alter or delete active or inactive transfers.
CCC_ADMIN_FACILITY	Defines users that can perform configure nodes and profiles via Command Center.

Parameter	Description
CCC_TRANSFER_FACILITY	Defines users that can initiate transfers via Command Center.
EXTENDED_SECURITY_CHECK	Defines whether extended RACF resource checking is performed to see if a user is authorized to initiate transfers through the TSO or BATCH interfaces. There is also a parameter that defines whether users are authorized to send files to particular nodes.
EXTENDED_SECURITY_CHECK_RESOURCE	Defines the Facility Class prefix used when EXTENDED_SECURITY_CHECK is enabled.
DNI_USERID	Defines the RACF user used when DNI scans for files to be transferred.
SAPI_USERID	Defines the RACF user used when SAPI scans for SYSOUT data to be transferred.

Miscellaneous Parameters

Parameter	Description
REQUIRE_NODE_DEFINITION	Allows you to require pre-defined nodes for initiator and responder requests.
RESPONDER_PROFILE	Sets the default that defines whether responder profiles are required. This parameter can be overridden by node definitions.
ACCEPT_VERIFIED_USER	We suggest using the default value of NO.
RESPONDER_PROFILE_LPASS	Defines if a local password is required when creating a responder profile for a local user that is different than the requestor's user ID.
TRANSFER_INTERFACE_PROTOCOL	Defines the protocol that can be used to initiate file transfers.
MANAGE_INTERFACE_PROTOCOL	Defines the protocol that can be used to manage

Parameter	Description
	configuration information.
ALLOW_TRANSFER_REQUESTS	Defines the default value for all nodes that define whether transfers can be initiated by a node. This parameter can be overridden by Node definitions.
ALLOW_MANAGE_REQUESTS	Defines the default value for all nodes that define whether configuration information can be initiated by a node. This parameter can be overridden by Node definitions.

Node Parameters

There are a variety of node parameters that affect security. For a more detailed description of these parameters, see the "Node Definition Parameters" section in *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*.

Security Parameters

Parameter	Description
ENFORCE_SECURITY_POLICY	<p>Defines the security policy for this node. Overrides the Global definition. You can configure the following values:</p> <p>FIPS140: STC is FIPS140 compliant.</p> <p>HIPAA: HIPAA rules requiring encryption are followed.</p>
RESPONDER_PROFILE	Overrides the Global Responder Profile setting.
ACCEPT_VERIFIED_USER	We suggest using the default value of NO.
DEFAULT_ENCRYPT	Defines the default encryption for initiator transfers with this node.

Parameter	Description
COMMAND_ CENTER_ SUPPORT	Defines whether requests from this IP address support Command Center functions.
ALLOW_ TRANSFER_ REQUESTS	Overrides the Global setting.
ALLOW_ MANAGE_ REQUESTS	Overrides the Global setting.
TLS	Defines whether communication to this node should be through TLS or Tunnel communication.

Execution of File Transfers

After you have installed and configured TIBCO MFT Platform Server for z/OS, you must set the transfer process parameters provided in the following section.

Transfer Process Parameters

There are a variety of transfer process parameters that affect security. For a more detailed description of these parameters, see "Defining the Batch Interface Parameters" in the *TIBCO® Managed File Transfer Platform Server for z/OS User's Guide*.



Note: When you want to use "User Profiles", set the remote user (RUSER) to *PROFILE. Example: RUSER=*PROFILE

Security Parameters

Parameter	Description
ENCRYPT	Defines the level of encryption for a transfer. Overrides the node definition.

Parameter	Description
TLS	Defines whether communication to this node should be through TLS or Tunnel communication.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [TIBCO Product Documentation](#) website, mainly in HTML and PDF formats.

The [TIBCO Product Documentation](#) website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for TIBCO® Managed File Transfer Platform Server for z/OS is available on the [TIBCO® Managed File Transfer Platform Server for z/OS Product Documentation](#) page.

- *TIBCO® Managed File Transfer Platform Server for z/OS Release Notes*
- *TIBCO® Managed File Transfer Platform Server for z/OS Managed File Transfer Overview*
- *TIBCO® Managed File Transfer Platform Server for z/OS Installation and Operation Guide*
- *TIBCO® Managed File Transfer Platform Server for z/OS Security Guide*
- *TIBCO® Managed File Transfer Platform Server for z/OS User's Guide*
- *TIBCO® Managed File Transfer Platform Server for z/OS Message Manual*

How to Contact TIBCO Support

Get an overview of [TIBCO Support](#). You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the [TIBCO Support](#) website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to [TIBCO Support](#) website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

Legal and Third-Party Notices

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, TIBCO Managed File Transfer, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, and TIBCO Managed File Transfer Platform Server are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2003-2021. TIBCO Software Inc. All Rights Reserved.