



TIBCO® Managed File Transfer Platform Server for UNIX

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 Mode	7
Miscellaneous Security Features	8
Security Tasks	10
Pre-installation	10
Installation and Configuration	11
Execution of File Transfers	15
Post Installation Tasks	16
TIBCO Documentation and Support Services	17
Legal and Third-Party Notices	19

Introduction

TIBCO® Managed File Transfer Platform Server for UNIX 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 UNIX. It provides security-related guidance and recommendations for installation, configuration, and execution of file transfers.

Security Features

TIBCO MFT Platform Server for UNIX provides many features that enhance security. Here is a summary of these features. These features are discussed in more detail later in the document.

- [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 executed the transfer:

- Initiator Transfers
- Responder Transfers

Initiator Transfers

For transfers initiated by TIBCO MFT Platform Server for UNIX:

- The user ID of the user initiating the transfer

For transfers initiated by TIBCO MFT Command Center:

- The user ID/password sent by Command Center

Responder Transfers

For transfers initiated by a Platform Server partner:

- When the CyberResp daemon is executing under root, the transfer executes under the transfer credentials sent by the initiator, or under the User ID defined in responder profiles. See *Password Management: Responder Profiles* for more

information.

- When the CyberResp daemon is executing under a non-root account, transfers run under the CyberResp UID.

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 UNIX Installation and Operation Guide* and the "SSL Authentication" section in *TIBCO® Managed File Transfer Platform Server for UNIX 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 UNIX supports 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 UNIX 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 can be used when the transfer has NOT defined user ID and password credentials for the remote system.
- Platform Server matches the user submitting the transfer and the target node defined for the transfer against user profile definitions created through the `cfprofile` command.
- 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.

Responder Profiles

Responder profiles are used when remote Platform Server clients initiate transfers to Platform Server for UNIX. The CyberResp daemon matches the credentials sent by the client against predefined responder profile credentials for that server. Here is how responder 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 cfrprofile command.
- When CyberResp is running as a root user and a match is found, the transfer is run under the rights of the local user associated with the responder profile.
- When CyberResp is running as a non-root user and a match is found, the transfer continues under the rights of the CyberResp process UID.

Advantages of Using Responder Profiles

- The credentials used to connect to Platform Server for UNIX cannot log on to the UNIX system.
- You can reduce the number of operating system user 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



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 `config.txt` Configuration section.

File Transfer Mode

TIBCO MFT Platform Server for UNIX 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.

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 *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide* in the section titled "Configured SSL Authorization Parameters". 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. SSLAUTH checking requires the `config.txt ClientVerification` set to Y.

CRL for TLS/SSL and Tunnel Transfers

The *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide* in the section titled "CRL Support" describes how to configure CRL Support.

However, it is simpler to update the `SSLAAuth` file to deny access to specific certificates.

Miscellaneous Security Features

TIBCO MFT Platform Server for UNIX includes two features, documented in the *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide*, that can limit access to UNIX files: `Access Control` and `CFALIAS`. Both of these features are supported for responder transfers only.

ACCESS Control

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
- Execute a command

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 these sections:

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

Pre-installation

Prior to installing TIBCO MFT Platform Server for UNIX, you must decide whether the responder daemon (CyberResp) runs as a root or a non-root account. Here is an explanation of the root and non-root installs:

Deciding whether to run as root or non-root is a decision that must be made by each customer based on their policies and requirements.

i Note: Initiator (Client) transfers run the same for root and non-root installs under the user that executes the transfer.

Here are the differences between a root and non-root installation.

ROOT Installation

- The CyberResp daemon runs as a root account.
- When a transfer or Command Center request executes, Platform Server verifies the credentials against the PAM, or the password/shadow password files, or responder profiles. For a successful log in, a `setuid` is executed for the transfer user ID.
- Transfers and management requests run under the UID of the transfer user.
- File authorization checking is performed under the transfer user's UID.

Non-ROOT Installation

- The CyberResp daemon runs under the UID of the process starting CyberResp.

- The `config.txt` `SERVER RequiredNodeDefinition` parameter is set to Yes. All incoming requests must have a corresponding Node definition.
- When a transfer or Command Center request executes, Platform Server verifies the credentials against the Responder Profiles.
- Validation against PAM or the system password or shadow password files is not supported.
- Transfers and management requests run under the `CyberResp` process UID. File authorization checking is performed under the `CyberResp` process UID.

Installation and Configuration

After you have installed TIBCO MFT Platform Server for UNIX, you must configure security-related parameters mentioned in the following sections based on your requirements:

- [config.txt Parameters](#)
- [Node Parameters](#)

config.txt Parameters

There are a variety of `config.txt` parameters that affect security mentioned in the following sections. For a detailed description of these parameters, see the "Configuration Parameters" in *TIBCO® Managed File Transfer Platform Server for UNIX Installation and Operation Guide*.

config.txt Security Parameters

Parameter	Description
SecurityPolicy	Defines the security policy for the Platform Server started task. You can configure the following values: NONE: No security policy is defined. FIPS140: STC is FIPS140 compliant. HIPAA: HIPAA rules requiring encryption are followed.

Parameter	Description
ClientVerification	For TLS/SSL transfer, client certificates are required.
AllowRoot	<p>Defines whether responder transfers can run under root. You can configure the following values:</p> <p>All: Allow transfers to run under root.</p> <p>N: Do not allow transfers to run under root.</p> <p>Password: Allow transfers to run under root if the root password is defined. The default value of N is recommended.</p>
PamAuth	Defines whether PAM authentication is used. Support for root installations only.
SemaphoreMaxWaitTime	Defines how long CyberMgr waits to complete. You may need to raise this value on high volume systems if you find that audit records (log.txt) are not being written.
RpcSynchIntervalHA	Defines the time range between the RPC client and RPC server that is honored. HA requires that the time is synchronized on RPC clients and RPC servers. If the times are not synchronized, you may need to increase the sync interval. This parameter is only needed when running in HA.
SSLEnabledProtocols	Defines the SSL/TLS protocols that are used. This parameter is defined in both the SERVER and CLIENT sections of the config.txt file.
Ciphers	Defines the SSL/TLS ciphers that are used. This parameter is defined in both the SERVER and CLIENT sections of the config.txt file.
Umask_Default	Defines the UNIX umask applied to the newly created files on the server. This is used for responder transfers only.
Uperm_Default	Defines the UNIX permissions set for newly created files on the server. This is used for responder transfers only.

Parameter	Description
CheckCRL	Defines whether CRL is checked for SSL/TLS transfers.
CAPath	Defines the path where the CRL checking looks for the hashed file names.
AccessControlConfig	Defines the fully qualified path of the Access Control Config files.
AliasConfig	Defines the fully qualified path of the Alias Config files.
RunCyberRespAsNonRoot	Defines whether you can run the CyberResp daemon as a non-root user.

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 cfrprofile utility or through Command Center.

- PasswordRuleChecking
- PasswordRequireUpperAndLower
- PasswordMinLength
- PasswordMinUnique
- PasswordMinNumber
- PasswordMinSpecial

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).

- ListenAdapterIP
- ListenAdapterIPv6

- ConnectAdapterIP
- ConnectAdapterIPv6

Group Class Checking Parameters

Parameter	Description
AdminGroup	Defines users that can create node definitions, user profiles, and responder profiles. Users can also inquire on completed transfers executed by any user.
BrowseGroup	Defines users that can inquire on completed transfers executed by any user.
TransferGroup	Defines users that can execute transfers initiated by Command Center.
StrictGroupChecking	Defines users that are granted rights assigned by membership in the group, if a group is not defined. This parameter defines whether requests should be denied if the group is not defined.

Miscellaneous Parameters

Parameter	Description
RequiredNodeDefinition	Allows you to require pre-defined nodes for initiator and responder requests. This parameter is defined in two places: SERVER: for Responder Transfers CLIENT: for Initiator Transfers
ResponderProfile	Sets the default that defines whether responder profiles are required. This parameter can be overridden by node definitions.
AcceptVerifiedUser	We suggest using the default value of No.

Node Parameters

There are a variety of node parameters that affect security. For a more detailed description of these parameters, see the "Transfer Using Nodes" section in *TIBCO® Managed File Transfer Platform Server for UNIX Installation and Operation Guide*.

Security Parameters

Parameter	Description
SecurityPolicy	Allows you to override the config.txt setting for transfers to this node.
ResponderProfile	Overrides the config.txt Responder Profile setting when running in root mode. For non-root mode, responder requests always validate against responder profiles.
AcceptVerifiedUser	We suggest using the default value of No.
Encrypt	Defines the default encryption for initiator transfers with this node.
CommandSupport	Defines whether requests from this IP Address supports Command Center functions.
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 UNIX, you must set the transfer parameters provided in the following section.

Transfer Parameters

There are a variety of transfer parameters that affect security. For detailed description of these parameters, see "Transfer Parameters" in the *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide*.

Security Parameters

Parameter	Description
ENCRYPT	Defines the level of encryption for a transfer. Overrides the node definition.
TLS	Defines whether communication to this node should be through TLS or Tunnel communication.
CRC	<p>Defines whether a Cyclic Redundancy Check (CRC) is performed for transfers initiated to this node.</p> <p>The valid values are:</p> <p>Yes: performs CRC checking.</p> <p>No: bypasses CRC checking.</p> <p>Default: uses CRC value from <code>config.txt</code></p>

Post Installation Tasks

For detailed information on how to change Platform Server file permissions and attributes, see *TIBCO® Managed File Transfer Platform Server for UNIX Installation and Operation Guide* under the section "Changing Ownership and Group Permissions".

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 TIBCO® Managed File Transfer Platform Server for UNIX is available on the [TIBCO® Managed File Transfer Platform Server for UNIX Product Documentation](#) page.

- *TIBCO® Managed File Transfer Platform Server for UNIX Release Notes*
- *TIBCO® Managed File Transfer Platform Server for UNIX Managed File Transfer Overview*
- *TIBCO® Managed File Transfer Platform Server for UNIX Installation*
- *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide*
- *TIBCO® Managed File Transfer Platform Server for UNIX Security Guide*
- *TIBCO® Managed File Transfer Platform Server for UNIX Docker Container Deployment*

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 Suite, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, 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.