



TIBCO® Managed File Transfer Platform Server for UNIX

Installation

*Version 8.1.0
August 2021*



Contents

Contents	2
Installation Overview	4
Installation Modes	4
Installation Environment	4
Installation Requirements	5
Installation Account	5
System Requirements	5
Group Requirements	5
Installation	8
Root and Non-Root Installation	8
Downloading the Software	9
Installing in Console Mode	10
Installing in Silent Mode	13
Example - silent.cfg File	15
Examples - Command-Line Installation	15
Installation Parameters	16
silent.cfg Parameters	17
Command-Line Parameters	20
Postinstallation Tasks	24
Setting the Required Environment Variables	24
Optional: Backing Up CyberMgr	25
Optional: Converting Regular Setup to High Availability Setup	26
Upgrading to a New Version	27
Considerations for Upgrading	27
Migrating Log.txt and transnum Files from the Old Version to the New Version	28

Upgrading Configuration Files from the Old Version to the New Version	33
Uninstallation	36
Uninstalling in Console Mode	36
TIBCO Documentation and Support Services	37
Legal and Third-Party Notices	39

Installation Overview

You can install TIBCO® Managed File Transfer Platform Server for UNIX with different accounts in different modes.

Installation Modes

You can install TIBCO Managed File Transfer (MFT) Platform Server for UNIX in console or in silent mode.

- **Console Mode**
In console mode, you can run the installation on a command line.
- **Silent Mode**
In silent mode, the installation can be completed without prompting you for information. You can type the required and supported parameters to run a silent installation.

Installation Environment

An installation environment isolates product installations. A product installed into an installation environment does not access components in other installation environments.

An installation environment is the top-level installation directory for TIBCO products. The installation environment consists of the following properties:

- **Directory**
Identifies the directory into which the product is installed.
- **Name**
Identifies the name of the folder where the product is installed.

The installation environment of TIBCO MFT Platform Server for UNIX is referenced as CFRROOT. For both root and non-root installations, the default value of CFRROOT is /mftps.

Installation Requirements

Before you run the installation, make sure that your system meets all the necessary hardware and software requirements and that you have the appropriate privileges to run the installation.

Installation Account

Any type of user, regular (non-root) user and super-user (root), can perform the installation. However, non-root installation requires additional node and profile configurations before you can perform any file transfers.

System Requirements

For information about the hardware and software requirements as well as supported platforms, see the product readme file.

Group Requirements

TIBCO MFT Platform Server uses three groups to perform different functions. By default, these groups are named as cfadmin, cftransfer, and cfbrowse.

See the following table for what each group is responsible for:

Group Name	Responsibility
cfadmin	A member of the cfadmin group can configure nodes, local profiles, responder profiles, as well as view audit records from all users.
cfbrowse	A member of the cfbrowse group can view audit records from all users.

Note: Users not in the cfbrowse or cfadmin group can only view transactions that their user ID performed.

Group Name	Responsibility
cftransfer	A member of the cftransfer group can perform platform-to-platform file transfers initiated from Command Center.
	Note: If the group does not exist when a transfer request comes from Command Center, the request is processed based on the node configurations for Command Center. However, when the group does exist, but the user who initiates a file transfer from Command Center is not a member of the group, the transfer fails.

See the following table for the group requirements for both installation methods. Y means that the group must exist before the installation; N means that the group is not required to exist before the installation.

Installation Method	cfadmin	cfbrowse	cftransfer
Root Installation	Y	N	N
Non-Root Installation	Y	N	N

- For the root installation:
 - The cfadmin group must exist in the system before the installation. Therefore, the permissions of the folders and files can be assigned to this group. It can either be a group that already exists or a new group (the group does not need to have any members in it).
 - The cfbrowse and cftransfer groups do not have to exist before the installation. You can create these groups during installation or later.
- For the non-root installation:
 - The cfadmin group must be created before the installation. You can create the cfbrowse and cftransfer groups after installation. The user running the installation has the ownership of all the installed folders and files and must be a member of cfadmin group.

i Note: The installation allows you to define group names that are different from the default group names. If you define different group names, the group names should not contain an embedded space. The group name defined as the `cfadmin` group must exist before the installation. After the installation, if you want to change any group name, you can modify the `config.txt` file located in the `$CFROOT/config` directory. You should also change the group associated with all files and folders in the `$CFROOT` directory.

For more information, see *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide*.

Installation

TIBCO MFT Platform Server for UNIX can be installed in console or in silent mode.

Make sure that your system meets all the requirements described in [Installation Requirements](#).



Note: TIBCO MFT Platform Server for UNIX can be installed in the same directory as prior versions of TIBCO MFT Platform Server for UNIX. However, since version 8.0.0, the directory structure has changed. Executable programs are now saved in the `$CFR00T/bin` directory. If you are upgrading from Platform Server 7.2.0 or before, you may need to update the `PATH` to set the correct directory.

If you install TIBCO MFT Platform Server for UNIX in a different directory than a prior installation, you must manually copy the configuration files. You also must update the `config.txt` file to set the configuration values. You should not use the `config.txt` file from a prior version.

Root and Non-Root Installation

Both root user and non-root user can perform the installation of TIBCO MFT Platform Server for UNIX. Transfers initiated by local users work the same for root and non-root installations. However, transfers initiated by a remote client work differently for root and non-root installations.

See the following table for the differences between root installations and non-root installations. This table only applies to responder requests.

Root Installation	Non-Root Installation
Supported authentication methods: <ul style="list-style-type: none">• Responder profiles authentication• TLS certificate authentication• Authentication using the password and shadow	Supported authentication methods: <ul style="list-style-type: none">• Responder profiles authentication• TLS certificate

Root Installation	Non-Root Installation
<p>password file</p> <ul style="list-style-type: none"> • PAM authentication <p>Note: For more information on configuring PAM authentication, see <i>PAM Authentication</i> in <i>TIBCO® Managed File Transfer Platform Server for UNIX User's Guide</i>.</p>	<p>authentication</p>
<p>Transfers are executed under the transfer user's credentials.</p> <ul style="list-style-type: none"> • When a responder profile is validated, a set UID is executed to set the transfer process to the UID associated with the responder profile. • When a user's credentials is validated, a set UID is executed to set the transfer process to the transfer user's credentials. 	<p>Transfers are executed under the credentials of the user who starts the CyberResp daemon.</p> <ul style="list-style-type: none"> • When a responder profile is validated, a set UID is not executed to set the transfer process to the UID associated with the responder profile.
<p>File authorization checking is performed under the transfer user's UID.</p>	<p>File authorization checking is performed under the UID of the user who starts the CyberResp daemon.</p>

Downloading the Software

To download the software from TIBCO Software Product eDelivery Site, you must enter a user name and password. If you do not have a user name and password, contact TIBCO Support.

Procedure

1. Download the package from the TIBCO download website: edelivery.tibco.com.
2. Unzip the package to a local directory.
3. Upload the installation package (example: TIB_mftps-unix&zlinux_v.v.v_linux.tar) in binary format to a temporary directory on the UNIX system.

There are multiple ways to upload the file to the UNIX system. For example, to use FTP to copy the package, you can use the following commands at the DOS command prompt:

```
ftp UNIX_machine_name/IP_address
cd /usr/tmp
bin
put "TIB_mftps-unix&zlinux_v.v.v_linux.tar"
bye
```

Installing in Console Mode

When installing in console mode, you can run the installation on the command line as either a root user or a non-root user. Note that if you use the non-root option, the following capabilities are not available to you:

- Validation of password against the UNIX security system.

Without this capability, responder profiles are required to provide authentication before any file transfers can be performed. To use the responder profiles, you have to create nodes. Each responder profile is associated with a node. For more information, see *TIBCO® Managed File Transfer Platform Server for UNIX User's Guide*.

- Executing responder transfers under the effective `userId` (UID) of the credentials sent by the transfer initiator.

Before you begin

You must download the product software. For instructions, see [Downloading the Software](#).

Procedure

1. Configure the UNIX system.
 - a. If you are a root user, log in to the UNIX system with the root account. Optionally, you can use `sudo` to install as a root user. Or, if you are a non-root user, log in to the UNIX system with the non-root account. It is good practice to install the software using the same non-root account which will be used to start the CyberResp daemon.
 - b. Create a `cfadmin` group with a suitable name using the `groupadd` command.

i Note: You must define this group before running the `install` or `install.noroot` script.

2. On the command line, navigate to the temporary directory where the installation package is located.
3. Use the `tar` command to extract the installation files.

```
tar -xvf mftps_tar_file_name
```

For example,

```
tar -xvf "TIB_mftps-unix&zlinux_v.v.v_linux.tar"
```

4. Run the `install` script if you are a root user or the `install.noroot` script if you are a non-root user by using the following command:

```
./install
```

or

```
./install.noroot
```

- a. Press Enter after you finish reading the license agreement, and then type Yes to accept the license agreement.
- b. Type Y or y to accept the default installation directory `/mftps`.
If you want to choose another directory, type N or n so you can enter an installation path. The new directory is created if it does not exist.
- c. Type Y or y if you are already collecting `Log.txt` transaction history from this machine.
- d. If you are installing in the same directory as a prior installation, type R or r to restore the existing configuration files or type N or n to bypass restoring the configuration files.

If you do not restore the existing configuration files, they are saved in folder: `$CFROOT/BACKUP_CONFIG`.

- e. Type Y or y to accept the default group names: cfadmin, cftransfer, and cfbrowse.
If you want to choose another group, type N or n so you can enter each group name. For more information, see [Group Requirements](#).
- f. Type Y or y if you want to create symbolic links in the /usr/lib directory for each file in the /libs directory.
- g. Type Y or y to create a Command Center (CC) node. Enter the node name, host, and port when prompted.
- h. If you want to choose installation with High Availability (HA), type Y or y.
 - Type Y or y if you want the configuration files to be used by all machines in the shared environment.
- i. In the final installation message:
 - Review the location of the configuration file (by default \$CFROOT/config). You can use the configuration file to configure server settings.
 - Review the three environment variables and update them as required.
 - CFRROOT: Defines the TIBCO MFT Platform Server for UNIX installation directory.
 - PATH: Defines the path where the TIBCO MFT Platform Server for UNIX executable programs are located.
 - LD_LIBRARY_PATH (or LIBPATH for AIX): Defines where runtime libraries are located.



Note: It is recommended to add the environment variables to your log in profile. These three environment variables must be set before executing any transfers or starting the TIBCO MFT Platform Server for UNIX Responder daemon.

Result

At the end, you receive an "Installation completed successfully" message. And all the executable programs, such as cfdi, cfinq, cfnode, cfprofile, cfrprofile, cfmutex, cfsend, cfrecv, cfstart, cfstop, substart, fusing, fusutil, startmgr, msgmgr, hainstall, CyberMgr, CyberMgrBackup, CyberResp are saved in the \$CFROOT/bin folder.

What to do next

See the [PostInstallation Tasks](#).

Installing in Silent Mode

When installing in silent mode, the installer does not prompt you for any input during the installation. As a root or non-root user, you can choose either to provide input in the `silent.cfg` file or on the command line for the silent installation. The `silent.cfg` file is included in the Platform Server distribution `.tar` file. This file allows you to define or configure all the parameters required for an installation.

Before you begin

You must download the product software. For instructions, see [Downloading the Software](#).

Procedure

1. On the command line, navigate to the temporary directory where the installation package is located.
2. Use the `tar` command to extract the installation files.

```
tar -xvf mftps_tar_file_name
```

For example,

```
tar -xvf "TIB_mftps-unix&zlinux_v.v.v_linux.tar"
```

3. For the silent installation, you can proceed in either one of the following ways:
4. If you want to use the `silent.cfg` file option for the silent installation, then enter the parameters in the file.

For information on supported parameters, see [Installation Parameters](#); or, for an example, see [Example - silent.cfg File](#).

Run the `install` script if you are a root user or the `install.noroot` script if you are non-root user by using either one of the following commands.

```
./install silent
```

or

```
./install.noroot silent
```

i Note: If you install using the silent configuration file, all files, including `silent.cfg`, are deleted at the end of the installation. You should make a backup copy of `silent.cfg` prior to running the install scripts so that the script can be used in subsequent installations.

5. If you want to use the command-line option for the silent installation, type the parameters that are required for a silent installation, that is, `-q` and `-accepteula`.

For information on supported parameters, see [Installation Parameters](#); or, for examples, see [Examples - Command-Line Installation](#).

Run the `install` script if you are a root user or the `install.noroot` script if you are non-root user by using the following command.

```
./install -q -accepteula  
./install.noroot -q -accepteula
```

6. Review the following information in the final installation message:
 - Location of the configuration file (by default `$CFROOT/config/config.txt`): you can use it to configure the default settings.
 - Path information: you can use it to configure the required environment variables. At the end of installation, you are promoted to update the `PATH` as `export PATH=$PATH:$CFROOT/bin`

Result

When the installation is completed, all the executable programs, such as `cfdir`, `cfinq`, `cfnode`, `cfprofile`, `cfprofile`, `cfmutex`, `cfsend`, `cfrecv`, `cfstart`, `cfstop`, `substart`, `fusping`, `fusutil`, `startmgr`, `msgmgr`, `hainstall`, `CyberMgr`, `CyberMgrBackup`, `CyberResp` are saved in the `$CFROOT/bin` folder.

What to do next

See the [PostInstallation Tasks](#).

Example - silent.cfg File

The following section provides an example of a silent.cfg file.

```
# This file defines the default Silent install parameters.
# To do a silent install, enter: ./install silent
# These parameter can be overridden by arguments on the command line.
# For more information, enter ./install -?
AcceptEula:           Yes                # Yes | No
InstallDirectory:     /mftps             # Install Directory
SaveAndRestoreConfig: Yes                # Yes | No | Save
CreateSoftLinks:      No                 # Yes | No
AdminGroup:           cfadmin            # Admin Group Name
BrowseGroup:          cfbrowse           # Browse Group Name
TransferGroup:        cftransfer         # Transfer Group Name
CCNodeName:           CCNode             # CC Node Name
CCNodeIPName:         CCNodeIPName       # CC IP Name
CCNodeIPPort:         46464              # CC IP Port
CCCollector:          Yes                 # Yes | No
HAMode:               No                 # HA Yes | No
HAResourceDirectory:  /Shared/HADirectory # HA Shared Directory
HAPrimaryRPCIPName:   primary.mftrpc.ip  # HA Primary RPC IP Name
HASecundaryRPCIPName: secondary.mftrpc.ip # HA Secondary RPC IP Name
HAPrimaryRPCPort:     46678              # HA Default Primary RPC Port
HASecundaryRPCPort:   46678              # HA Default Secondary RPC Port
HAUseMyConfigFiles:   Create             # HA Create | Replace | No
```

Examples - Command-Line Installation

Example 1:

```
./install -q -accepteula -ugr -d /opt/mftps -ulnk
```

This example is set up to accept the license agreement, the default cfadmin, cfbrowse, and cftransfer group names. Choose the /opt/mftps directory as the installation directory, and create a soft link to point to the \$CFROOT/libs directory.

Example 2:

```
./install -q -accepteula -ugr -agr MFTAdmins -d /opt/mftps -ulnk
```

This example is set up to accept the license agreement, change the default cfadmin group name to MFTAdmins, keep the default cfbrowse and cftransfer group names. TIBCO MFT

Platform Server for UNIX is installed in the `/opt/mftps` directory and a soft link is created to point to the `$CFROOT/libs` directory.

Example 3:

```
./install -q -accepteula -ugr -d /opt/mftps -ulnk -ccnode cc_node_name cc_
node_host cc_node_port
```

This example is set up to accept the license agreement, the default `cfadmin`, `cfbrowse`, `cftransfer` group names, and to create a CC node. Choose the `/opt/mftps` directory as the installation directory, create a soft link to point to the `$CFROOT/libs` directory, and enter the CC node name, host, and the port.

Example 4:

```
./install -q -accepteula
-ugr -d /opt/mftps -ulnk
-ccnode CCNode CC.YourOrg.com 46464
-hamode -dshared /shared/directory
-hprimary primaryrpcipname:46678
-hsecondary secondaryrpcipname:46678
-cfiles r
```

This example is set up to accept the license agreement, the default `cfadmin`, `cfbrowse`, `cftransfer` group names, and to create a CC node. Choose the `/opt/mftps` directory as the installation directory, create a soft link to point to the `$CFROOT/libs` directory, and create the CC node with name `CCNode`, hostname `YourOrg.com` and port number `46464`. HA mode is then enabled. The directory that is shared with other HA Platform Server instances is: `/shared/directory`. The primary and secondary RPC name parameters point to the CyberMgr instances on the primary and secondary HA cluster instances. `-cfiles r` indicates that the config files from the installation directory will overwrite the config files in the HA shared directory.

Installation Parameters

The installation parameters are organized under the following sections:

- [silent.cfg Parameters](#)
- [Command-line Parameters](#)

silent.cfg Parameters

The following table lists the parameters supported in the `silent.cfg` file.

Parameter	Description
AcceptEula	Defines whether you have accepted the EULA (End User License Agreement). <ul style="list-style-type: none">• Yes: You have read and accepted the EULA.• No: You have not accepted the EULA. The installation is terminated.
InstallDirectory	Defines the installation directory for the Platform Server.
SaveAndRestoreConfig	When installing over an existing Platform Server installation, it defines whether to save and restore the configuration files. <ul style="list-style-type: none">• Yes: Saves and restores configuration files.• No: Overwrites the configuration files.
CreateSoftLinks	Defines whether you want to create soft links for the run-time libraries in the <code>/usr/lib</code> directory. <ul style="list-style-type: none">• Yes: Creates soft links for the run-time libraries in <code>/usr/lib</code>. This parameter is only allowed when installing in root mode.• No: Does not create soft links. Use the <code>LD_LIBRARY_PATH</code> (or <code>LIBPATH</code> on AIX) to define where the runtime libraries are located.
AdminGroup	Defines the name of the admin group. The default admin group name is <code>cfadmin</code> .
BrowseGroup	Defines the name of the browse group. The default admin group name is <code>cfbrowse</code> .
TransferGroup	Defines the name of the transfer group. The default transfer group name is <code>cftransfer</code> .

Parameter	Description
CCNodeName	<p>Defines the name of the CC node that is created at the end of the installation. When this parameter is not defined, the CC node is not created.</p> <p>Note: Ensure that CCNodeName does not have spaces in it.</p>
CCNodeIPName	Defines the IP name or IP address of the CC node that is created at the end of the installation.
CCNodeIPPort	Defines the IP port of the CC node that is created at the end of the installation.
CCCollector	<p>Defines whether Command Center (CC) is already collecting Log.txt transaction history from this machine. cccollector must be defined on upgrade, when there is already another PSU instance installed on the machine. If this is a brand new installation or an upgrade into an existing folder, the cccollector parameter can be omitted altogether because there is no potential issue with CC collecting Log.txt transaction history from this machine.</p> <ul style="list-style-type: none"> • Yes: CC Collector is already collecting log records from this machine. If a user is already collecting logs from the machine but installing version 8.1.0 in a different folder, the cccollector value should be yes. In this case, at the end of installation, there is a message to reset CC Collector server for the machine. • No: CC Collector is not collecting log records from this machine. If a user is not collecting logs from the machine, but installing version 8.1.0 in a different folder, the cccollector value should be no. In this case, there is no collector messages at the end of installation.

Parameter	Description
	<p>Note: This parameter is defined to let the silent installer know that collection is being performed and that the user may need to copy the Log.txt files to the new log file directory.</p>
HAMode	<p>Defines whether HA is enabled by this installation.</p> <ul style="list-style-type: none"> • Yes: HA mode is enabled. • No: HA mode is not enabled (Default). <p>Note: HA Mode can be configured via hainstall script after the installation is over. When Yes is defined, the HA parameters below must be defined.</p>
HASharedDirectory	Defines the name of the HA shared directory. This directory must be accessible for read/write access to all Platform Server instances in the HA cluster.
HAPrimaryRPCIPName	Defines the IP name or IP address of the primary CyberMgr daemon. When running in an HA cluster, the HAPrimaryRPCIPName and HASecondaryRPCIPName parameters must be defined in the same order for all Platform Server instances in a cluster.
HASecondaryRPCIPName	Defines the IP name or IP address of the secondary CyberMgr daemon. When running in an HA cluster, the HAPrimaryRPCIPName and HASecondaryRPCIPName parameters must be defined in the same order for all Platform Server instances in a cluster.
HAPrimaryRPCPort	Defines the IP port of the primary CyberMgr daemon.
HASecondaryRPCPort	Defines the IP port of the secondary CyberMgr daemon.
HAUseMyConfigFiles	Defines whether to copy the configuration files in the local installation to the shared configuration directory.

Parameter	Description
	<ul style="list-style-type: none"> • Create: Copies the configuration files but does not replace existing files. (Default) • Replace: Copies the configuration files to the shared directory. If there are already files in the shared directory, they are replaced. Backup of replaced files is available. • No: Does not copy the configuration files to the shared directory.

Command-Line Parameters

The following table lists the parameters supported by the `install` command in alphabetical order.

Parameter	Usage
<code>-accepteula</code>	Accepts the End User License Agreement.
<code>-agr</code>	Defines the name for the Admin group.
<code>-bgr</code>	Defines the name for the Audit Browse group.
<code>-c</code>	Saves and restores configuration files during a re-installation.
<code>-ccnode</code>	<p>Defines the Command Center node. You must enter the fields in the following format:</p> <pre>-ccnode cc_node_namecc_node_host cc_node_port</pre>
<code>-cfiles</code>	<p>Defines the configuration files. Only one of the options below can be set.</p> <p>c - Copies the configuration files but does not replace existing files. (Default) " " (use this server's configuration files only if there are no existing configuration files in the shared HA environment).</p> <p>r - Replaces the configuration files. The server configuration files are used</p>

Parameter	Usage
	in the shared HA environment. n - Does not copy the server configuration files. The server configuration files are not used in the shared HA environment.
-d	Defines the directory where TIBCO MFT Platform Server for UNIX is installed.
-dshared	Defines the directory path accessible by all machines.
-h or -?	Displays help.
-hprimary	Defines the host name for the primary RPC service.
-hsecondary	Defines the host name for the secondary RPC service.
-n	Saves but does not restore configuration files during a re-installation.
-q	Uses the default installation options. Does not ask any questions. Runs the script in silent mode without user input.
-tgr	Defines the name for the Transfer group.
-ugr	Configures special group names.
-u1nk	Creates links in the /usr/lib directory for files in the \$CFR00T/libs directory.

Parameter	Usage
	<p>Note:</p> <p>When using the <code>uLnk</code> parameter:</p> <ul style="list-style-type: none"> • The <code>install.noroot</code> script does not support the <code>uLnk</code> parameter because root rights are required to create these links. • Soft links are created in the <code>/usr/lib</code> directory for each file in the <code>\$CFROOT/libs</code> directory. • If a soft link that points to the files in the <code>\$CFROOT/libs</code> directory already exists in the <code>/usr/lib</code> directory, a link is not created. In this case, you have to set the <code>LD_LIBRARY_PATH</code> environment variable before using TIBCO MFT Platform Server for UNIX. • You must be careful when you create links for different versions of TIBCO MFT Platform Server for UNIX. If the <code>lib</code> files are not in the <code>/usr/lib</code> directory, you can require <code>LD_LIBRARY_PATH</code> for different versions of TIBCO MFT Platform Server for UNIX.
<code>-cccollector</code>	<p>Defines whether Command Center (CC) is already collecting <code>Log.txt</code> transaction history from this machine. <code>cccollector</code> must be defined on upgrade, when there is already another PSU instance installed on the machine. If this is a brand new installation or an upgrade into an existing folder, the <code>cccollector</code> parameter can be omitted altogether because there is no potential issue with CC collecting <code>Log.txt</code> transaction history from this machine.</p> <ul style="list-style-type: none"> • Yes: CC Collector is already collecting log records from this machine. If a user is already collecting logs from the machine but installing version 8.1.0 in a different folder, the <code>cccollector</code> value should be yes. In this case, at the end of installation, there is a message to reset CC Collector server for the machine. • No: CC Collector is not collecting log records from this machine. If a user is not collecting logs from the machine, but installing version 8.1.0 in a different folder, the <code>-cccollector</code> value should be no. In this case, there is no collector message at the end of installation.

Parameter	Usage
	Note: This parameter is defined to let the silent installer know that collection is being performed and that the user may need to copy the Log.txt files to the log file directory.
-hamode	<p>Defines that HA mode is enabled for this installation. You must enter the fields in the following format.</p> <pre>-hamode -dshared shareddirectory -hprimary primaryrpcipname -hsecondary secondaryrpcipname -cfiles c r n</pre> <p>The -cfiles option is the same as HAUseMyConfigFiles in the silent.cfg file.</p>

Postinstallation Tasks

After installing TIBCO MFT Platform Server for UNIX, you must perform the postinstallation tasks as required to ensure that you can use this product smoothly.

- [Setting the Required Environment Variables](#)
- [Optional: Backing Up CyberMgr](#)
- [Optional: Converting Regular Setup to High Availability Setup](#)

Setting the Required Environment Variables

You can set the required variables at the time of installation or at a later time before you run any Platform Server commands.

TIBCO MFT Platform Server requires correct configuration of the following environment variables. These variables must be set for all users who run TIBCO MFT Platform Server. Use the `export` statements provided in the message at the end of the installation to set correct values for these variables.

Parameter	Description
CFROOT	Used by TIBCO MFT Platform Server for UNIX to locate the installation directory.
PATH	Used by UNIX to locate the platform server executables.
LD_LIBRARY_PATH	Used by UNIX to locate the necessary <code>lib</code> files.

Note: For AIX system, you must set the `LIBPATH` environment variable.

You can define these environment variables by using one of the following approaches:

- In the system profile: you can configure the default value for all users.
- In the user profile: the user profile value overrides the system profile and becomes the default option for the user.

- On the command line: the command line overrides the system profile and user profile.

i Note: It is good practice that you put these export statements in the user profile, otherwise you have to export PATH and CFR00T every time you log on.

For example, if you install TIBCO MFT Platform Server for UNIX to the default location, configure your variables as follows:

```
export CFR00T=/mftps
export PATH=$PATH:$CFR00T/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$CFR00T/libs
```

- i Note:**
- If you are running on AIX system, set your LIBPATH environment variable with the following command:
`export LIBPATH=$LIBPATH:$CFR00T/libs`
 - If you are running other applications that use `libstdc++` and `libgcc` files, do not run the `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$CFR00T/libs` command, or add it to the system profile or user profile.

Optional: Backing Up CyberMgr

After the installation is completed, CyberMgrBackup is included in the bin folder, which is a soft link to CyberMgr. If the CyberMgr process shuts down, CyberMgrBackup takes over until CyberMgr is restarted by running the startmgr script. This feature is merely a matter of convenience, and it does not provide any functionality gain.

i Note: The CyberMgrBackup feature only works in a non-HA setup.

Procedure

1. Run the backupinst script and this secondary daemon becomes available.
The backupinst script reconfigures your existing \$CFR00T environment to have two RPC daemons, CyberMgr and CyberMgrBackup. cfstart and cfstop starts and stops

both CyberMgr and CyberMgrBackup processes. (If you want to uninstall this feature, run `backupuninst`).

Optional: Converting Regular Setup to High Availability Setup

HA installation is available only in CLI mode. The `hainstall` script that is provided in version 8.1.0 can convert an existing regular product setup to HA setup. The script has the same CLI arguments as the `-hamode` portion of a regular installation.

i Note: This script should only be used when you want to enable High Availability and Platform Server is installed with `HAMode=No`. If you installed Platform Server with `HAMode=Yes`, you do not need to run this script.

The HA installation makes changes in your `$CFROOT` environment to support HA mode.

Procedure

1. Enter the arguments and run the script.

```
./hainstall [-dshared DirName] [-hprimary HostName] [-hsecondary  
HostName] [-cfiles c|r|n] [-q]
```

The secondary Platform Server is no different than any other Platform Server in an HA cluster, except that its CyberMgr RPC daemon is used if the CyberMgr RPC daemon on the primary Platform Server fails. For more information on the HA parameters, see "Command-Line Parameters" in [Installation Parameters](#).

i Note: The time on all Platform Server servers in an HA cluster should be synchronized.

Upgrading to a New Version

When upgrading the TIBCO MFT Platform Server for UNIX installation from an earlier version, you can run the `install` script and the output is similar with the regular installation.

For information on other points to consider before upgrading to the new version, see [Considerations for Upgrading](#) section.

Procedure

1. On the command line, navigate to the installation directory.
2. Run the `install` script by using the following command.

```
./install
```

3. Type `Y` to reinstall TIBCO MFT Platform Server for UNIX.

If you type `N` or `n` here, the installer prompts you to remove the directory where you want to install TIBCO MFT Platform Server for UNIX first and try the installation again.

4. Type `R` or `r` to restore your old configuration files.

If you type `N` or `n`, your old configuration files are backed up and placed in a folder called `$CFROOT/BACKUP_CONFIG`.

The installation proceeds as the regular installation after this step. For more information, see from Step 5e in [Installing in Console Mode](#).



Note: TIBCO MFT Platform Server versions till V8.0.0 installed the executable programs in the `$CFROOT` directory. After V8.0.0, the executable programs are installed in the `$CFROOT/bin` directory.

Considerations for Upgrading

When upgrading TIBCO MFT Platform Server for UNIX from an older version to a newer one in a different directory than a previous version, there are two issues that need to be

considered:

1. Migrating Log.txt files and the transnum (transaction number) file from the old version to the new version.
2. Upgrading configuration files from the old version to the new version.

In addition, TIBCO MFT Platform Server for UNIX now supports High Availability (HA). To support HA Platform Servers, configuration files are moved to a new directory that is accessible to all Platform Server instances in the HA cluster.

Migrating Log.txt and transnum Files from the Old Version to the New Version

TIBCO MFT Platform Server for UNIX writes an audit record for each completed transfer to the following file:

```
$CFR00T/log/Log.txt.yyyymmdd
```

Each transfer, whether successful or unsuccessful, is written to this log file. There are two ways to inquire on this log file:

1. Platform Server `cfinq` Utility
2. Command Center Audit Poll or Collection

When you install TIBCO MFT Platform Server for UNIX over an existing installation

When you install the new version of TIBCO MFT Platform Server for UNIX in an existing installation directory, the Log.txt files will remain; you do not need to do anything.

When TIBCO MFT Platform Server for UNIX is installed in a new directory

When you install the new version of TIBCO MFT Platform Server for UNIX in a new installation directory, there are no log files in the log directory. This causes two problems:

1. The `cfinq` utility is not be able to view any transfers from the old installation directory.
2. Command Center Collection fails. This is a more serious issue because many companies use Collection as a critical part of the process flow.

There are two approaches to resolving the collection problem:

- Approach 1: Copying Log and Transaction Number files
- Approach 2: Resetting the Collection History

Approach 1: Copying Log.txt and transnum Files

Before starting the new TIBCO MFT Platform Server CyberResp daemon, perform the following procedure:

1. Stop the CyberResp daemon on the old TIBCO MFT Platform Server version. (You must not use this version anymore).
2. Copy the transnum file from the old TIBCO MFT Platform Server to the new TIBCO MFT Platform Server to ensure that there are no duplicate transaction numbers.
3. Copy or move the Log.txt files from the log directory of the old version to the log directory of the new version. You can copy/move all of the files, or you can copy/move only the last few days.

Result

After doing this:

- The cfinq utility is able to view the audit records from previous versions of TIBCO MFT Platform Server.
- Command Center Collections continues to work and no audit records is lost. This assumes that Command Center Collection is configured for the IP port of the new TIBCO MFT Platform Server.

Approach 2: Resetting the Collection History

Before upgrading the TIBCO MFT Platform Server, you can perform the following procedure:

1. Make sure that all platform transfer records have been collected by the Command Center. (If you are migrating to HA mode, make sure that all audit records have been collected on both Platform Servers).
2. Stop the old version of TIBCO MFT Platform Server.
3. Copy the transnum file from the old version to the new version of TIBCO MFT Platform Server to ensure that there are no duplicate transaction numbers.
4. Stop the Collector.

5. Go to the Command Center Update Server page for the new TIBCO MFT Platform Server.
6. Click the **Management Options** tab.
7. Select the **Reset Collection History** check box.
8. Click **Update** to update the server definition.
9. Start the Collector.

Collection is then started for all transfers completed by the new TIBCO MFT Platform Server.

i Note: This approach requires TIBCO MFT Command Center to be at the 8.2.1_HF-002, 8.3.0_HF-001, or 8.4.0 level.

High Availability Considerations

Platform Server High Availability (HA) allows two or more Platform Servers to act as a single Platform Server. When using HA mode, Platform Servers are set up to use a shared directory for the log and configuration files.

Here are some items that should be considered when implementing HA mode:

- You can migrate any PS server to HA mode by either running the `install` script or by running the `hainstall` script.
- When you run the `install` script, you can install a new PSU 8.1.0 or upgrade your existing version to version 8.1.0, and at the end of installation you are asked whether or not you want to proceed migrating to the HA mode right away.
- You can upgrade an existing PSU version 8.1.0 from a regular mode to HA mode at any time by running the `hainstall` script from the `$CFROOT/bin` folder.

Upgrading the First Platform Server to the HA Cluster

When you upgrade the first Platform Server to the HA cluster, follow a procedure based on the approach you choose:

Make sure you know the IP Name of the primary and secondary Platform Servers. The first Platform Server migrated to the HA Cluster should be the primary Platform Server.

Approach 1: Copying Log and Transnum Files

Procedure

1. Run the `install` script or the `hainstall` to convert to HA mode, indicate your PS machine as a primary one.
2. Manually copy or move log files from old log folder to a new one on the shared drive.
3. If you are installing TIBCO MFT Platform Server 8.1.0 over an existing version, the config files and transnum file are copied to the common HA config directory.
4. If you re installing a brand new TIBCO MFT Platform Server 8.1.0, the default config files and transnum file are copied to the common HA config directory.
5. If you are installing TIBCO MFT Platform Server 8.1.0 in a directory different from your existing Platform Server, you should manually copy the config files to the common HA config directory. Otherwise, you have only a default configuration files in the common HA folder. You should also manually copy or move the old transnum file to a new `trn` folder on a shared drive.
6. You do not need to change any Collection setting on Command Center Server definition side, unless you plan to use the Load Balancer (LB) which is in front of this new Platform Server running in HA Mode. If you plan to use LB with your new HA cluster, then reconfigure the Command Center Server definition to point to the IP name and port of the LB.

Approach 2: Resetting the Collection History

Before migrating to HA mode, make sure that all platform transfer records have been collected by Command Center.

Procedure

1. Stop the old version of TIBCO MFT Platform Server.
2. Run the `install` script or the `hainstall` to convert to HA mode, indicate your PS machine as the primary one.
3. If you are installing TIBCO MFT Platform Server 8.1.0 over an existing version, the config files and transnum file are copied to the common HA config directory.
4. If you are installing a brand new TIBCO MFT Platform Server 8.1.0, the default config files and transnum file are copied to the common HA config directory.

5. If you are installing TIBCO MFT Platform Server 8.1.0 in a directory different from your existing Platform Server, you should manually copy the config files to the common HA config directory. Otherwise, you must have only a default configuration file in the common HA folder. You must also manually copy or move the old transnum file to a new trn folder on a shared drive.
6. If you want to use the Load Balancer (LB) with your new HA cluster, then re-configure the Command Center Server definition to point to the IP name and port of the LB. Also, you must select the **Reset Collection History** check box. Or, if you do not plan to use LB with your new HA cluster, then the only thing you must do on the Command Center Server definition is to clear the **Reset Collection History** check box.

After your first Platform Server is migrated to HA mode, you can add other Platform Servers to the HA Cluster by running the `install` or the `hainstall` script on those machines. However, do not designate the new Platform Servers as a “Primary”. Their existing configuration files are not used in HA mode. If you do not want to lose transaction history from those machines, make sure that all log records are collected by Command Center Collector before HA migration.

Upgrading Additional Platform Servers to the HA Cluster

When you add additional Platform Servers to the HA cluster, follow this procedure:

Procedure

1. Use the same IP name and port for the primary and secondary Platform Servers that you used when migrating the primary Platform Server to the HA cluster.
2. Point the additional Platform Servers to the same configuration parameters that the primary HA Server uses. For more information, see [High Availability Considerations](#). (Additional Platform Servers use the same transaction number and audit log files that the primary HA Server uses. So, you do not need to copy any config, transnum, or log files).
3. Run the `install` or the `hainstall` script to install the new server in HA mode, and define the same primary and secondary HA server IP name that was used in the Primary HA installation.

After additional Platform Servers are added to HA cluster, their respective Command Center Server definitions should be deleted. Only one “Server Definition” is needed per HA cluster.

Upgrading Configuration Files from the Old Version to the New Version

TIBCO MFT Platform Server has a variety of configuration files that it uses.

Here is a list of the TIBCO MFT Platform Server configuration files.

Config File	Description
config.txt	Defines Client, Server, and Common configuration parameters for the Platform Server. This file, or a link to the file, must be in the \$CFROOT/config directory. This file defines the location of all other config files.
AccessControl.cfg	Defines configuration for Access Control. The config.txt AccessControlConfig parameter defines the path of this file.
CfAlias.cfg	Defines configuration for the CfAlias feature. The config.txt AliasConfig parameter defines the path of this file.
cfcos.cfg	Defines the Class of Service file. The config.txt ConfigDirectory parameter defines the location of this file.
CfgPostProc.cfg	Defines Configuration for the configured post processing feature. The CfgPostProc parameter in config.txt defines the path of this file.
cflist.cfg	Defines the distribution list file. The ConfigDirectory parameter in config.txt defines the location of this file.
cfnode.cfg	Defines the node definition file. The ConfigDirectory parameter in config.txt defines the location of this file.
cfprofile.cfg	Defines the profile definition file. The ConfigDirectory parameter in config.txt defines the location of this file.
cfrprofile.cfg	Defines the responder profile definition file. The ConfigDirectory parameter in config.txt defines the location of this file.
SSLAuth.cfg	Defines configuration for the Responder SSL Authorization file. The AuthorizationFileName parameter in config.txt defines the path of this file.

When you install TIBCO MFT Platform Server for UNIX over an existing installation

The installer prompts you to restore configuration files. If you choose **Y**, the installation does not overwrite the existing configuration files; they are upgraded and remain in the `$CFROOT/config` directory. If you choose **N**, the configuration files are copied to a backup directory and the installation overwrites the existing configuration files with the default configuration files.

When TIBCO MFT Platform Server for UNIX is installed in a new directory

You should manually copy all configuration files (except the `config.txt` file) from the old Platform Server `config` directory to the new Platform Server `config` directory after the installation is completed. For files that are configured in the `config.txt` (`AccessControl.cfg`, `CfAlias.cfg`, `CfgPostProc.cfg`, `SSLAuth.cfg`), make sure that they are using the standard names and that the `config.txt` file for the new version uses the same paths as the old version. Note that these files are not required and are not frequently used.

i Note: Never copy the `config.txt` to the new TIBCO MFT Platform Server for UNIX installation. The `config.txt` files are not forward or backward compatible; instead, manually update the `config.txt` file in the new TIBCO MFT Platform Server for UNIX installation, if needed.

High Availability Considerations

Platform Server High Availability (HA) allows two or more Platform Servers to appear as a single Platform Server to clients. All Platform Servers in the Platform Server "cluster" use the same configuration files.

Here are some items that should be considered when implementing HA mode:

- Each Platform Server that is a cluster member must have its own `$CFROOT/config/config.txt` file.
- The `HADirectory` parameter in the `config.txt` file must point to a common directory accessible to all Platform Servers in the HA cluster.
- The `ConfigDirectory` parameter in `config.txt` file must point to a directory with common configuration files under the defined `HADirectory`.

- Configuration files from one of the Platform Servers (usually defined as the “primary one”) must be copied to the HA ConfigDirectory. (The only exception is if you are running the `install` script and upgrading your old primary Platform Server to the new version with a different `$CFROOT`. Then, you will have to copy configuration files from your old `$CFROOT/config` to HA ConfigDirectory directory manually).

The Command Center Server definition for the cluster typically should point to a Load Balancer that directs requests to one of the Platform Servers. When the Command Center adds, deletes, or updates a configuration entry, the updated configuration applies to all Platform Servers in the HA cluster.

i Note: Load balancers can ping CyberResp daemon on any machine in HA setup. The Load Balancer should not connect to CyberMgr port on any machine in HA setup. CyberMgr is an RPC server, listening and waiting for RPC requests. The Load Balancer pinging it causes an interruption and delays of overall Platform Server functionality.

i Note: All HA configuration entries in the `$CFROOT/config/config.txt` must be identical for each Platform Server in the HA cluster. For example, if you changed `HACyberMgrSecondary` entry in one of the `config.txt` files, all other cluster instance `config.txt` files must be updated with the same value. Otherwise, you can have duplicate transaction numbers and corrupted log files.

If you have several Platform Servers in a cluster, manually updating all `config.txt` files can become error prone. You can do the following to simplify this:

Procedure:

1. Stop all Platform Server responders by running the `cfstop` script.
2. Move the `config.txt` (typically from the primary machine) from `$CFROOT/config` to HA ConfigDirectory folder.
3. Rename `$CFROOT/config/config.txt` on all other Platform Servers. You need not use them anymore.
4. In the `$CFROOT/config` folder on each Platform Server, create a soft link, pointing to `config.txt` in HA ConfigDirectory folder.
5. Start all Platform Servers; they will use the same shared `config.txt`.

Uninstallation

You can uninstall TIBCO MFT Platform Server for UNIX in console mode.

Uninstalling in Console Mode

To uninstall this product, use the `uninstall` script that is provided in the `$CFROOT` directory.

Procedure

1. On the command line, navigate to the `$CFROOT` directory.
2. Stop the Platform Server Responder and CyberMgr. Run the `cfstop` command.

```
cfstop
```

If SSL mode was started, then run the following command.

```
cfstop -ssl
```

If tunnel mode was started, then run the following command.

```
cfstop -tunnel
```

When the last CyberResp daemon is stopped, the CyberMgr daemon is also stopped.

3. Run the following command to start the uninstallation:

```
uninstall
```

4. Type Y to remove TIBCO MFT Platform Server for UNIX and all its components.

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.