TIBCO® Managed File Transfer Internet Server

Managed File Transfer Overview

Version 8.4.1
February 2022

Copyright © 2003-2022. TIBCO Software Inc. All Rights Reserved.

Contents

Contents **2**

TIBCO® Managed File Transfer Components **4**

Sample MFT Deployment **5**

Detailed Explanation of TIBCO MFT Components **6**

MFT Command Center **7**

Supported Functionality in MFT Command Center 7

MFT Command Center Extends Capabilities of MFT Internet Server 8

MFT Command Center Extends the Capabilities of MFT Platform Servers 8

Other MFT Command Center Capabilities 9

MFT Internet Server **10**

Supported Functionality in MFT Internet Server 11

Supported Protocols in MFT Internet Server 11

MFT Internet Server Security Capabilities 12

MFT Internet Server Postprocessing Actions 14

Connection Manager **16**

Components of Connection Manager 16

Connection Manager Installation 16

Installation - Simple Architecture 17

Installation - Complex Architecture 18

Installation - Two Tier DMZ Architecture 18

MFT Platform Server **20**

MFT Platform Server Features 20

MFT Platform Server High Availability 22

MFT Platform Server Preprocessing and Postprocessing Actions 22

Event Driven Processing in MFT Platform Servers 23

pDNI **24**

pDNI Features 24

Interface to Other TIBCO Products **26**

Sample Transfer Flows **28**

TIBCO Documentation and Support Services **31**

Legal and Third-Party Notices **33**

TIBCO® Managed File Transfer Components

TIBCO® Managed File Transfer (MFT) includes the following major functional components that facilitate the secure transfer of data through a network.

- **MFT Command Center**

  It is used to configure and manage MFT Internet Server and MFT Platform Servers.

- **MFT Internet Server**

  It is used to perform file transfers, generally through the internet with open protocols such as SFTP, FTP, HTTPS, AS2, and the proprietary Platform Server protocol.

- **Connection Manager**

  It allows MFT Internet Server running in the DMZ to open all ports from the internal network to the external network.

- **MFT Platform Server**

  It is used to perform file transfers, generally in the internal network. MFT Platform Servers are developed for each platform and use a proprietary protocol.

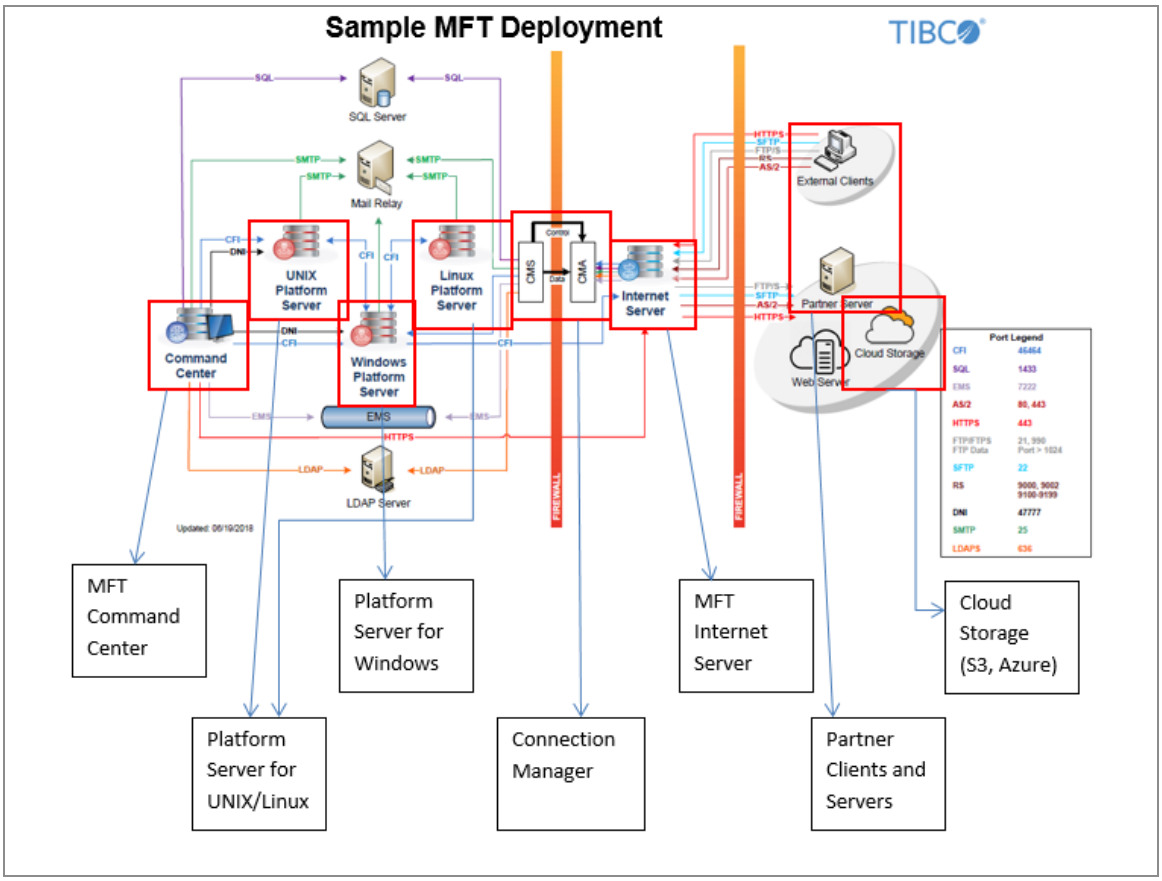
- **pDNI**

  It is an event-driven service that performs file transfers when a file is created or modified.

Each functional component is either a TIBCO product or a part of a TIBCO product. For more information about each component, see Detailed Explanation of TIBCO MFT Components.

Sample MFT Deployment

Here is a diagram of a typical MFT deployment.



Detailed Explanation of TIBCO MFT Components

Each of these TIBCO MFT components are discussed in detail in the following sections.

- MFT Command Center
- MFT Internet Server
- Connection Manager
- MFT Platform Server
- pDNI

MFT Command Center

MFT Command Center is a TIBCO® Managed File Transfer Command Center product.

MFT Command Center is the management component for MFT Internet Server and MFT Platform Servers. You can use the administrative component in MFT Internet Server to configure all of the parameters (users, servers, transfers) that executes file transfers. MFT Command Center extends these capabilities to provide additional functionality.

MFT Command Center runs in the internal network; it should not execute in the DMZ because you can configure and execute Internet Server transfers and Platform Server transfers.

Note: For any recent changes in MFT Command Center, see this section in the latest version of *TIBCO® Managed File Transfer Command Center - Managed File Transfer Overview*.

Supported Functionality in MFT Command Center

By default, MFT Command Center includes support for the following functions:

1. High Availability (HA). The MFT Scheduler and JMS interface work in a HA Active/Active environment.
2. LDAP or Database authentication
3. OIDC and SAML SSO (Single Sign On) support
4. Certificate and/or password authentication
5. APIs
    - REST calls to perform many configuration capabilities.
    - Command line interface to perform many configuration capabilities.
6. Logging and reporting of all administration changes (includes before and after images of the changes).

MFT Command Center Extends Capabilities of MFT Internet Server

MFT Command Center extends the capabilities of MFT Internet Server to perform the following functions:

1. Alerts: With alerts, you can configure actions based on events or non-events. There are three types of alerts:
    - Transfer Events: Alerts can be triggered by a transfer.
    - Non-Transfer Events: Alerts can be triggered by a transfer not executing.
    - Logon: Alerts can be triggered by a user logon.
2. Connection Manager Nodes: Connection Manager allows MFT Internet Server instances running in the DMZ to open all connections from the internal network to the external network. For more information, see Connection Manager.
3. JMS Interface: The JMS interface allows you to initiate Internet Server or Platform Server transfers. Also provides a mechanism for MFT Internet Server to write data to, or read data from, JMS queues.
4. View Active Internet Server Transfers: MFT Command Center allows you to view transfers executing on all Internet Server instances in the MFT cluster.
5. Logging of all Admin Changes: This includes before and after images of the changes.

MFT Command Center Extends the Capabilities of MFT Platform Servers

MFT Command Center also extends the capabilities of MFT Platform Servers to perform the following functions:

1. Collection Service: It provides a centralized location for collecting and reporting on MFT Platform Server transfers. Also allows you to execute alerts when an MFT Platform Server transfer is collected.
2. Execute Platform Transfers: It allows platform transfers to be initiated from a centralized location.
3. Configure MFT Platform Servers: It allows you to configure the following MFT

Platform Server components:

- Node definitions
- Profiles and responder profiles

4. View Active Platform Server Transfers: MFT Command Center allows you to view transfers executing on defined MFT Platform Server instances. Note that this capability requires MFT Platform Server V8.1 or higher.

Other MFT Command Center Capabilities

MFT Command Center also includes the following management capabilities:

1. Reporting: It allows you to execute reports on transfers, users, alerts, and AS2 transfers.
2. Status Server: It displays the status of target servers that MFT Internet Server communicates with.
3. Scheduler: It allows you to schedule the following actions:
    - Perform Platform Server transfers
    - Perform Internet Server transfers
    - Send emails
    - Execute commands
    - Execute Java class
    - Perform maintenance functions
    - Notify users of expiring keys
    - Purge database tables
    - Purge log files
4. DNI Daemons: DNI Daemons allow you to manage pDNI templates from a centralized location. For more information, see Event Driven Processing in MFT Platform Servers.

MFT Internet Server

MFT Internet Server is the TIBCO® Managed File Transfer Internet Server product.

MFT Internet Server is the file transfer component. MFT Internet Server supports many open protocols, and it also supports the Platform Server protocol. MFT Internet Server has an administrative component that allows you to configure all of the parameters (users, servers, transfers) to allow file transfers to execute. For additional capabilities, you can install MFT Command Center.

MFT Internet Server can be installed in the DMZ or in the internal network; when executing in the DMZ, you must disable the administrative capability because it allows you to configure Internet Server transfers.

Think of MFT Internet Server as a protocol converter. Here is an example:

- **File Upload**

  An SFTP client connects to MFT Internet Server to upload a file. The MFT Internet Server is configured to send the file to a target MFT Platform Server:

  SFTP --> Internet Server --> Platform Server for Linux

  As MFT Internet Server receives packets from the SFTP client, it converts the packets to the Platform Server protocol and sends the packets to the MFT Platform Server. All of this is done in a streaming mode. Packets are not written to a disk file; the file can be sent directly to the location where the data is processed.

- **File Download**

  An HTTP client connects to MFT Internet Server to download a file. The MFT Internet Server is configured to receive the file from a target FTPS Server:

  HTTPS <-- Internet Server <-- FTPS Server

  As MFT Internet Server receives packets from the FTPS Server, it converts the packets to the HTTPS protocol and sends the packets to the HTTPS client. All of this is done in a streaming mode. Packets are not written to a disk file; the file can be sent directly from the location where the file is stored.

Note: For any recent changes in MFT Internet Server, see also the latest version of *TIBCO® Managed File Transfer Internet Server - Managed File Transfer Overview*.

Supported Functionality in MFT Internet Server

By default, MFT Internet Server supports the following functions:

1. High Availability (HA). Because MFT configuration information is stored in the database, MFT Internet Server runs HA Active/Active.
2. High volume. Each Internet Server can run hundreds of concurrent transfers.
3. LDAP or Database authentication
4. SAML support
5. Certificate/Key and/or password authentication
6. APIs
    - REST calls to perform many configuration capabilities.
    - REST calls to perform file transfers.
    - Command Line interface to perform many configuration capabilities.
7. Logging of all admin changes. Includes before and after images of the changes.
8. Mailbox capability. Allows you to upload a file to an MFT repository and send an email to the end user. When the end user clicks on a link in the email, they can download the file from the MFT repository (after logging in and being authenticated).
9. File sharing capability. Users can share directories with other users.
10. Postprocessing actions

Supported Protocols in MFT Internet Server

MFT Internet Server supports the following client protocols:

1. FTP, FTPS

2. SFTP
3. HTTP/HTTPS(through a browser client or an API)
4. AS2
5. Platform Server Protocol

MFT Internet Server supports protocols for connecting to the following target servers:

1. FTP, FTPS
2. SFTP
3. Platform Server (Proprietary Protocol)
4. HTTP/HTTPS Server
5. AS2
6. Amazon S3 Buckets
7. Custom Server
8. Azure File Share, Block Blob, or ADLS Gen2 Storage
9. JMS Server
10. Local Accessible Storage (I.e. NAS or NFS)
11. HDFS
12. Google Cloud Storage or BigQuery Storage
13. OFTP2 Servers
14. Microsoft SharePoint Servers
15. Mailbox Servers
16. Email Servers

MFT Internet Server Security Capabilities

MFT Internet Server ensures the security of file transfers and the file transfer data by implementing the following capabilities:

1. PGP Encryption/Decryption: MFT can PGP-encrypt or PGP-decrypt data in a streaming

mode. PGP provides the following capabilities:

a. It provides non-repudiation. MFT can identify the signature of the client that encrypted and signed the data.

b. PGP provides an extra level of encryption. Clear text FTP transfers can send encrypted data that can only be decrypted by a PGP client with the correct private key.

c. This adds a second level of security to secure protocols. For example, you can PGP encrypt data send in an encrypted SSH connection. This provides two high levels of encryption.

d. PGP can also automatically compress and decompress data.

When transferring sensitive data or data that contains financial transactions, we strongly suggest using double levels of encryption: SFTP and PGP.

2. Key/Certificate and/or Password authentication: Key/Certificate authentication provides the highest level of authentication security. The client key or certificate associated with the private key must be uploaded to MFT and associated with a user before it can be used. Hence, only users with the client system key and the system key password can connect to MFT. Key/Certificate is supported for the following protocols:

   a. Platform Server protocol

   b. HTTPS

   c. FTPS

   d. SFTP

   Client connections to MFT servers support key/certificate authentication.

   MFT connections to target servers also support key/certificate authentication.

3. Rights assignments: MFT provides granular rights to allow specific admin or transfer functionality. No access is allowed if you do not have the required rights.

4. Password lockout functionality: MFT can be configured to lockout users after a pre-defined number of invalid logon attempts.

5. File transfer access: No access is allowed by default. `TransferRight` must be assigned to a user before any transfers can be performed. Additionally, transfer definitions must be defined for a user before any transfers can be performed.

6. User configuration: A user can be configured so that the user can upload files without

getting access to see any files or directory lists.

7. Virtual aliases: The actual location of the files and directories is abstracted from the end user through the use of virtual aliases. For example, the following definitions can be made for a user:
    - Tax data can be located on a target UNIX Platform Server.
    - Payroll can be located on a target UNIX SFTP Server.
    - Invoices can be located on a customer's FTPS Server.
8. File uploads and downloads: Data can be pulled (download) from a target server or pushed (upload) to a target server. This allows MFT to initiate all file transfers for and from a target customer. MFT also allows the customer to initiate upload or download transfers.

MFT Internet Server Postprocessing Actions

MFT Internet Server provides the following support for postprocessing actions:

- Postprocessing is defined in the transfer definition.
- Up to four postprocessing actions can be defined.
- All postprocessing actions are executed on MFT Internet Server or on a target server.
- Each postprocessing action can be executed on success or failure.
- The following postprocessing commands are supported:
    - Execute command
    - CALLJCL (MFT Platform Server for z/OS only)
    - CALLPGM (MFT Platform Server for z/OS only)
    - SUBMIT (MFT Platform Server for z/OS only)
- Up to 256 bytes of data can be passed to the postprocessing action. Symbolic parameters can be used to pass transfer-related information to the Postprocessing data field.
- When the target server is a Platform Server, the post processing actions are passed directly to the target Platform Server.
- When the target server is a Local Server, the postprocessing actions are executed on

the Internet Server.

- When the target server is an FTP/FTPS Server, the postprocessing actions are limited to `Delete` or `Rename` commands.
- When the target server is an SFTP Server, the postprocessing actions are limited to `Delete` or `Rename` commands. In addition to `Delete` or `Rename`, there is a special format of the PPA that can execute commands on a target SFTP Server.

Connection Manager

Connection Manager is a part of the TIBCO® Managed File Transfer Command Center product.

Connection Manager is used together with MFT Internet Server when Internet Server is running in the DMZ. Many installations do not allow TCP connections to be opened from the DMZ network to the internal network. Connection Manager solves this problem by opening all connections from the internal network to the external network.

Components of Connection Manager

There are two components to Connection Manager:

1. Connection Manager Server: Runs in the internal network. Establishes control connections to the Connection Manager Agent. Accepts a connection request from the Agent over the control connection and creates TCP Connections to the Agent.
2. Connection Manager Agent: Runs in the DMZ. Requests connections over the control connections and accepts connection request from the Connection Manager Server.

Connection Manager Agent is shipped with MFT Internet Server. Connection Manager Server is distributed with MFT Command Center. MFT Command Center is required to configure the Connection Manager Agent and Server.

Connection Manager Installation

When MFT Internet Server is installed in the DMZ, it typically requires connections to servers in the internal network. This can include the following servers:

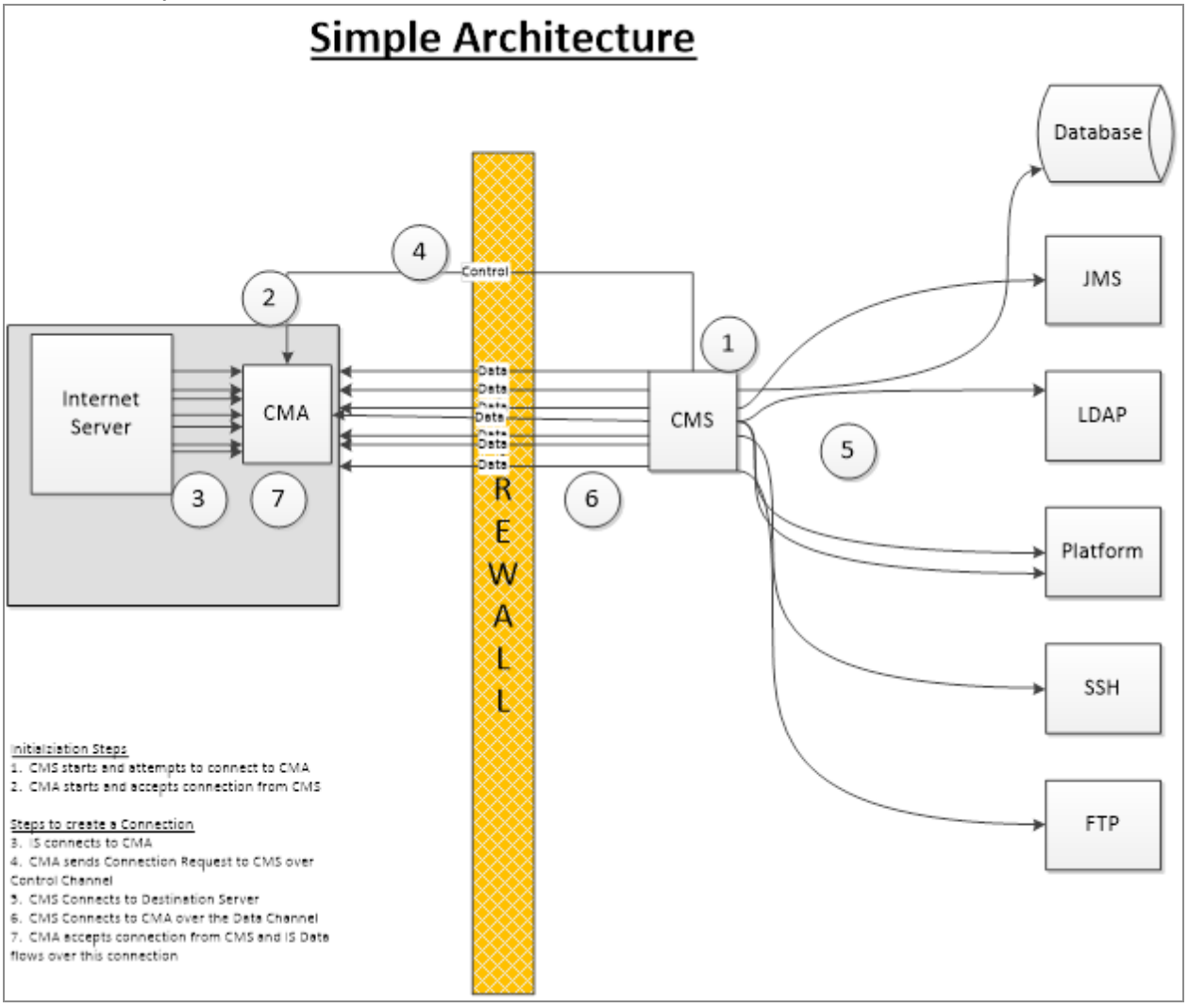
- LDAP Server
- JMS Server
- Platform Servers
- SMTP Servers
- SSH Servers

- FTP/FTPS Servers

Without the Connection Manager, MFT Internet Server must be able to open TCP connections from the DMZ to the internal network. Connection Manager. With the Connection Manager, you can open all TCP connections from the internal network to the DMZ. Firewalls frequently need exceptions to allow connections to be opened from the DMZ to the internal network.

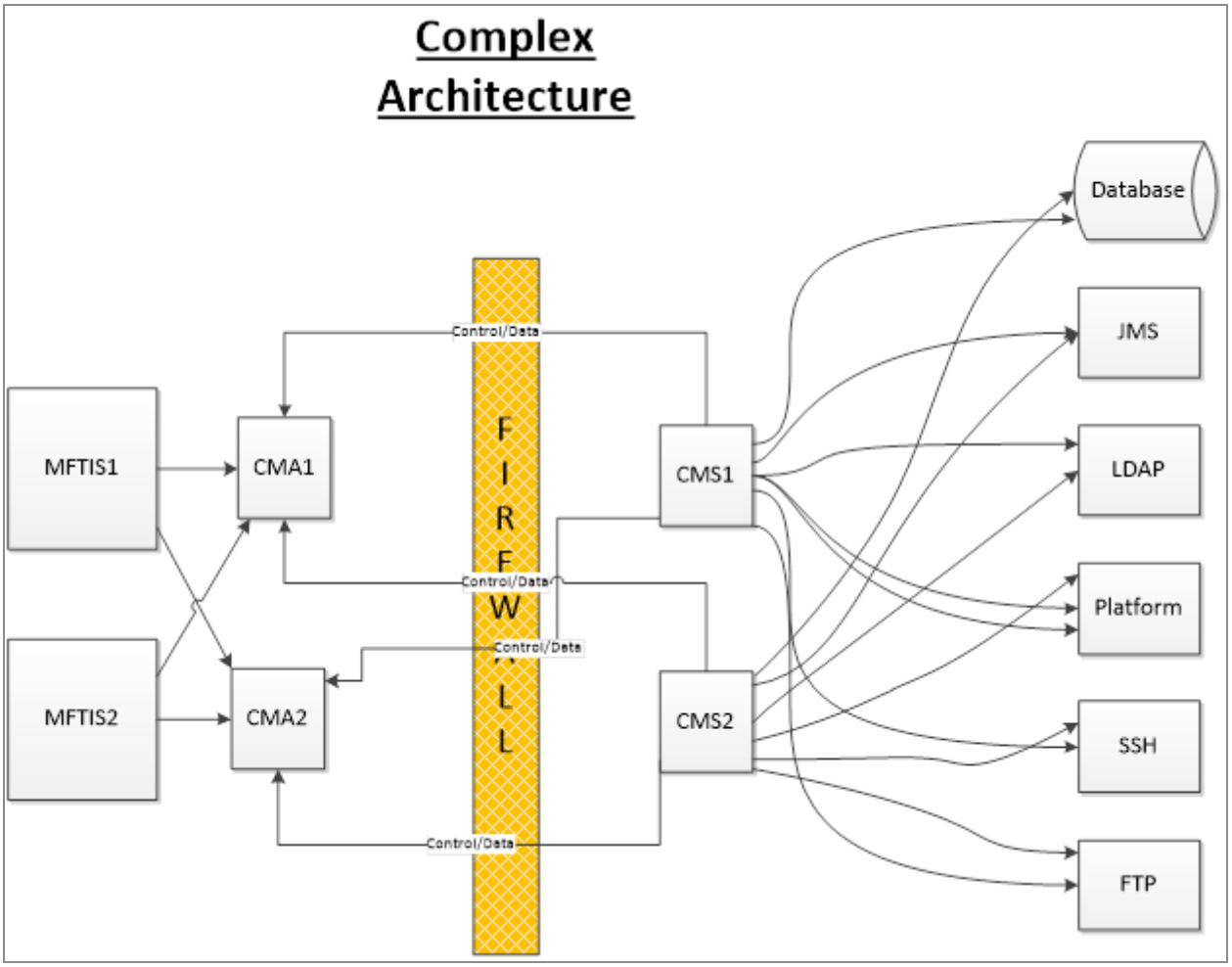
Installation - Simple Architecture

This example shows a simple Connection Manager installation. Internet Server needs to access multiple servers in the internet network (Database, JMS, LDAP, and so on).



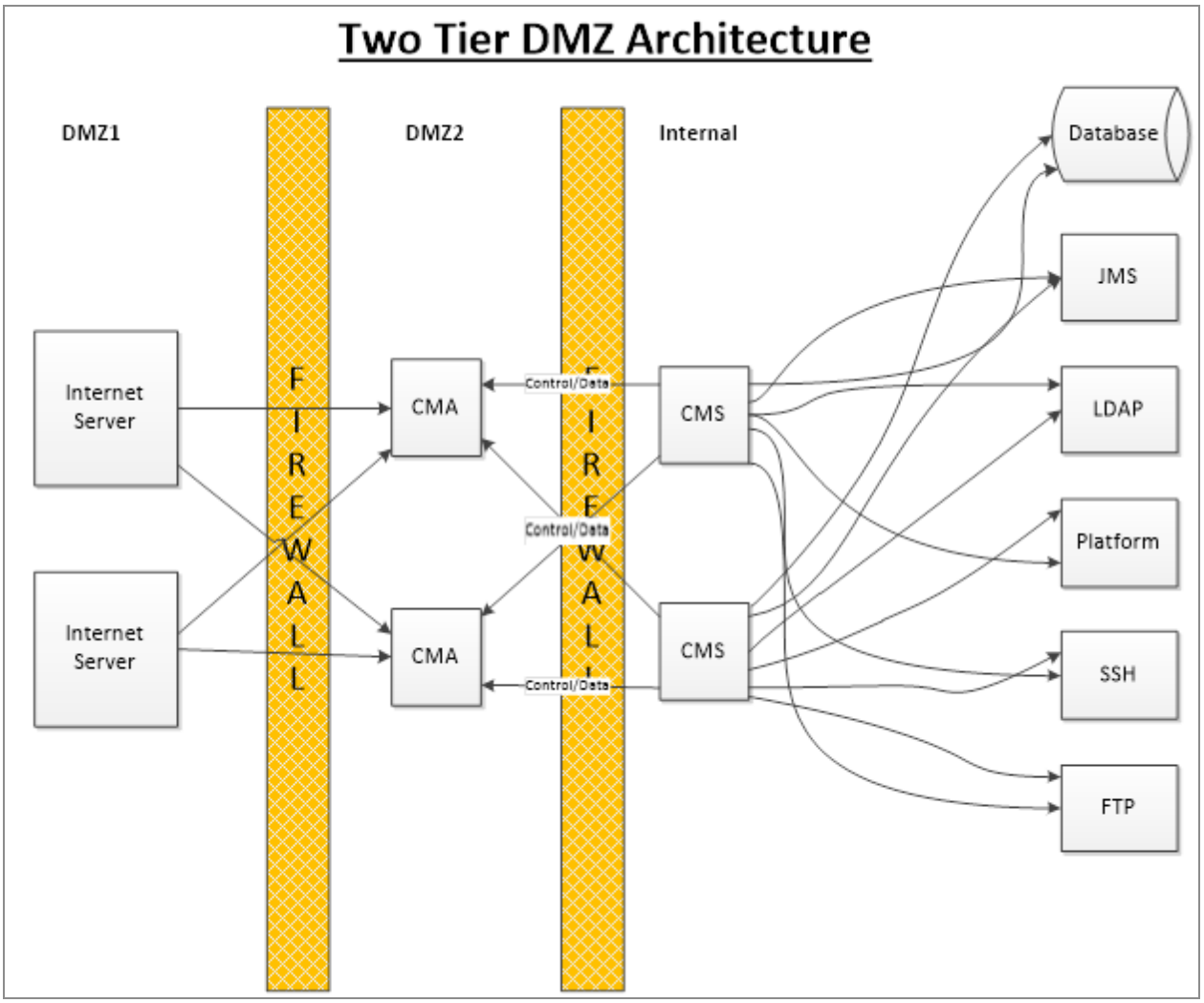
Installation - Complex Architecture

This example shows a complex Connection Manager installation. Note that the Internet Server machines are connected to multiple Connection Manager Agents (CMA). The Connection Manager Agents have connections to multiple Connection Manager Servers (CMS).



Installation - Two Tier DMZ Architecture

This example shows a two tier Connection Manager installation. Note that for this to work, the Internet Server in DMZ1 must be able to initiate connections to the Connection Manager Agents in DMZ2. Connections between DMZ2 and the internal network are initiated by the Connection Manager Server.


Two Tier DMZ Architecture
DMZ1
DMZ2
Internal
Internet Server
Internet Server
FIREWALL
CMA
CMA
Control/Data
Control/Data
Control/Data
FIREWALL
CMS
CMS
Database
JMS
LDAP
Platform
SSH
FTP

MFT Platform Server

MFT Platform Server is available as TIBCO® Managed File Transfer Platform Server for UNIX, TIBCO® Managed File Transfer Platform Server for z/Linux, TIBCO® Managed File Transfer Platform Server for z/OS, TIBCO® Managed File Transfer Platform Server for Windows, and TIBCO® Managed File Transfer Platform Server for IBM i products.

MFT Platform Servers are peer-to-peer file transfer servers that typically execute in the internal network. MFT Platform Servers are built specifically for each platform. These servers are meant for high-volume transfers so they are efficient and fast. The following hardware and software platforms are supported:

Hardware

- Solaris SPARC
- Solaris Intel

Software

- Z/OS
- Windows
- IBM i
- z/Linux
- Linux
- AIX

Note: The Platform Server Agent (PSA) is a simple client and server that provides limited Platform Server capabilities for hardware/software platforms that do not support the Platform Server. The main requirement is a directory structure similar to UNIX, and support for Java version 1.5 or later.

MFT Platform Server Features

MFT Platform Servers have the following features:

1. They use a proprietary protocol to transfer files.
2. They can initiate a file send or a file receive to a target Platform Server.
3. They can initiate a directory send or directory receive from a target Platform Server.
4. They can initiate a file send or file receive to a target Internet Server.
5. They can initiate a directory send or directory receive from a target Internet Server.
6. They support the following levels of data encryption:
    a. Use no data encryption.
    b. Use AES 256 encryption.
    c. Use a TLS session to negotiate symmetric keys for AES 256 encryption.
    d. Encapsulate all data through TLS tunnel.
7. They allow multiple ways to authenticate and pass credentials.
    a. User profiles allow users to transfer files without knowing the target system credentials.
    b. Responder profiles allow users to transfer files without providing any credentials to the target Server.
8. When using TLS or Tunnel Mode, they allow you to configure the software to accept only specific certificates.
9. When running on z/Linux, Linux, or UNIX, the Platform Server Daemon can run as root or non-root.
10. When running on Windows, requests can be validated against the responder profiles or Active Directory.
11. When running on z/Linux, Linux, or UNIX requests can be validated against the responder profiles or the password or shadow password files. PAM authentication is also supported.
12. Command Center can manage some Platform Server functionality, such as the following functions:
    a. View completed Platform Server transfers.
    b. View and update node definitions.
    c. View and update profile and responder profile definitions.

    d. Execute a transfer.

13. They can perform postprocessing actions when a transfer completes. This is discussed in more detail later in this document.
14. They can run a command on a target system.
15. They can send an email when a transfer completes, either successfully or unsuccessfully.
16. Perform authorization using the security of the UNIX or Windows platform.

MFT Platform Server High Availability

MFT Platform Server for UNIX, Linux, and z/Linux supports high availability. When running behind a load balancer, two or more Platform Servers look like a single Platform Server to the transfer client.

MFT Platform Server Preprocessing and Postprocessing Actions

Preprocessing actions define the action that can be taken before a transfer starts. Based on the return code from the preprocessing action, transfer can continue, terminate, or be retried at the next retry interval. Preprocessing requires Platform Server V8.1 or higher. Preprocessing is not supported on Internet Server.

Postprocessing actions define the action that should be taken when a transfer completes, either successfully or unsuccessfully. Postprocessing actions are supported on all Platform Servers. Limited postprocessing actions are also supported on Internet Servers as well.

- Up to four preprocessing and postprocessing actions can be defined.
- Preprocessing and postprocessing are defined on the command line or in the transfer process statements.
- Each preprocessing or postprocessing action can be executed in the initiator or the responder.
- Each postprocessing action can be executed on success or failure.

The following preprocessing and postprocessing commands are supported:

- Execute command
- CALLJCL (MFT Platform Server for z/OS only)
- CALLPGM (MFT Platform Server for z/OS only)
- SUBMIT (MFT Platform Server for z/OS only)

Up to 256 bytes of data can be passed to the preprocessing or postprocessing action. Symbolic parameters can be used to pass transfer related information to the Preprocessing or Postprocessing data field.

Event Driven Processing in MFT Platform Servers

MFT Platform Servers have some support for event-driven processing through the DNI (Directory Named Initiation) feature. Here is an overview of DNI capabilities integrated with MFT Platform Server.

Note: The pDNI (perl DNI) capabilities are described in more detail in the "pDNI" section.

- MFT Platform Server for z/OS DNI

  MFT Platform Server for z/OS supports initiating transfers based on the creation of a file. Because z/OS does not include a date-modified on its files, MFT Platform Server for z/OS cannot initiate transfers based on a file being modified. MFT Platform Server for z/OS DNI can also detect data in an MQ queue and initiate data transfer from the MQ queue to a target system.

- MFT Platform Server for Windows

  MFT Platform Server for Windows includes an integrated DNI capability that can be managed by the MFT Platform Server for Windows Administrator.

  MFT Platform Server for Windows also supports the pDNI that is described in the "pDNI" section.

- MFT Platform Server for z/Linux and UNIX

  MFT Platform Server for z/Linux and UNIX supports the pDNI that is described in the "pDNI" section.

pDNI

pDNI is a part of TIBCO® Managed File Transfer Platform Server for UNIX, TIBCO® Managed File Transfer Platform Server for z/Linux, and TIBCO® Managed File Transfer Platform Server for Windows products.

pDNI is a Perl based event-driven processing that works with these products.

pDNI Features

pDNI has the following features:

1. Monitor directories to detect files created or modified.
2. Wait for a predefined interval before sending and receiving a file to make sure that a file has not been modified.
3. Support for the following functionalities:
    a. DNI Send: Sends files to a target location.
    b. DNI Receive: Send files from a target location.
    c. FTP Receive: Receives files from an FTP Server (specifically the MFT Internet Server FTP Service).
4. Monitor subdirectories.
5. It supports High Availability in an Active/Passive mode.
6. It supports file and directory REGEX to limit the files transferred.
7. It supports directory scanning based on day of the week and time of the day.
8. It supports pre-transfer commands to limit the files that are transferred.
9. DNI Send and DNI Receive can execute any command; the default is to execute a cfsend/cfrecv(UNIX) or ftmscmd(Windows). But it allows you to execute any script or command.
10. It can execute up to 15 transfers at the same time.
11. Many DNI templates can run at the same time on a server. The only limit is the size of

the machine where pDNI is executing.

pDNI can be configured manually on each machine. In addition, pDNI can be configured from a centralized Command Center. pDNI supports a daemon that allows the following functionality:

1. Add, update or delete pDNI templates.
2. Start pDNI templates.
3. Stop pDNI templates.
4. View Template log files.

Interface to Other TIBCO Products

TIBCO MFT interfaces with TIBCO® EMS and TIBCO ActiveMatrix BusinessWorks™. Below is an explanation of the interfaces supported.

ActiveMatrix BusinessWorks™

TIBCO MFT has plug-ins for ActiveMatrix BusinessWorks™, that is for both TIBCO Business Studio™ (BW6) and TIBCO Designer™ (BW5). The plug-ins support the following capabilities:

1. Initiate a Platform Server transfer.
2. Wait for a Platform Server transfer to complete.
3. Initiate an Internet Server transfer.
4. Wait for an Internet Server transfer to complete.
5. Inquire on Internet Server or Platform Server audit records.
6. Wait for alerts.

The plug-ins are not shipped with ActiveMatrix BusinessWorks™ or with any TIBCO MFT product. You must download these plug-ins from the TIBCO download site and then install and configure them in ActiveMatrix BusinessWorks™ before they can be used.

The plug-in interface uses EMS (or other JMS Servers) as a pipe for receiving data from and sending data to the ActiveMatrix BusinessWorks™ client. Therefore EMS (or other JMS Servers) are required for ActiveMatrix BusinessWorks™ clients to work.

To use EMS or JMS, the MFT Command Center is required. Only MFT Command Center can configure EMS/JMS connections.

TIBCO EMS (or JMS)

You can use TIBCO Managed File Transfer to interface with EMS or other supported JMS products such as ActiveMQ or IBM MQ. The following capabilities are supported through EMS/JMS:

1. The following features are available from ActiveMatrix BusinessWorks™:
    a. Initiate a Platform Server transfer.

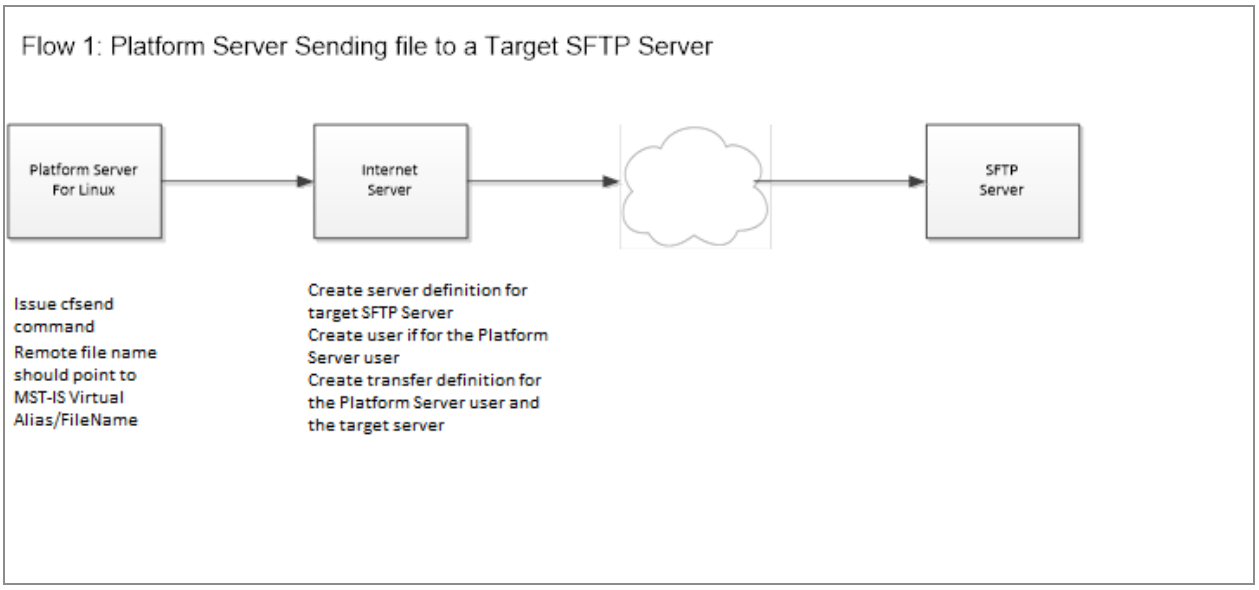
   b. Wait for a Platform Server transfer to complete.
   c. Initiate an Internet Server transfer.
   d. Wait for an Internet Server transfer to complete.
   e. Inquire on Internet Serve or Platform Server audit records.
   f. Wait for alerts.
2. Write file transfer data to an EMS/JMS queue, instead of to a file.
3. Read file transfer data from a EMS/JMS queue, instead of from a file.
4. Write transfer start (Internet Server) notifications to a topic.
5. Write transfer completion (Internet Server and Platform Server) notifications to a topic.

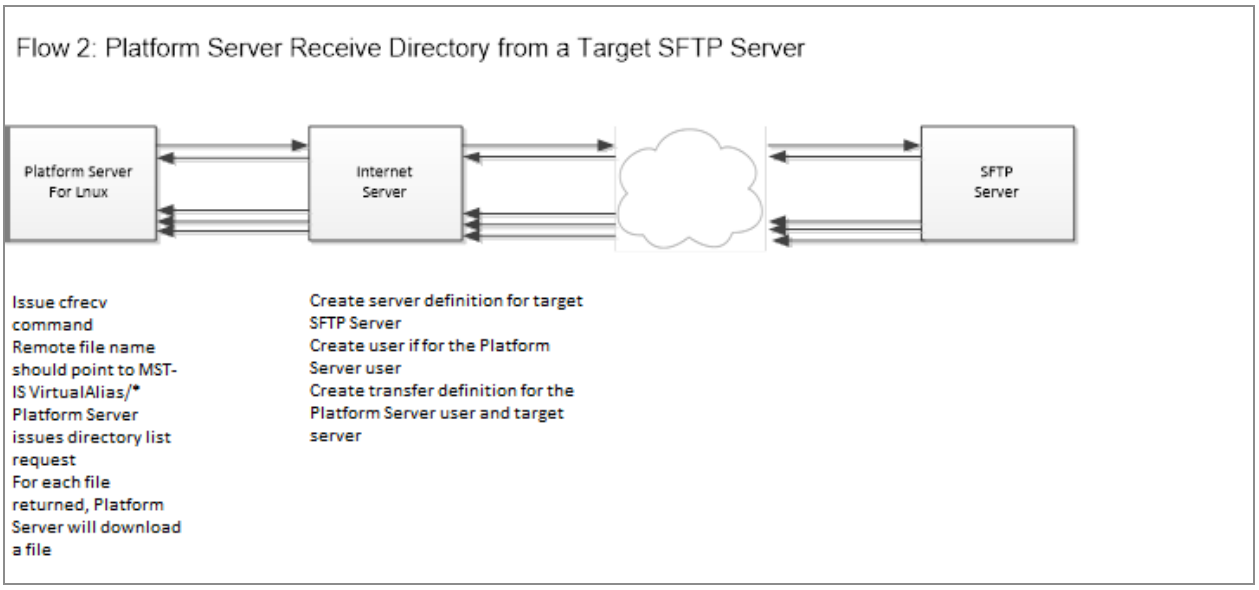
TIBCO Spotfire® and TIBCO JasperReports®

TIBCO MFT does not have a direct interface to Spotfire® or TIBCO JasperSoft®, but these products can be used to create sophisticated reports above and beyond the reports created by MFT Command Center. All MFT configuration and audit information is stored in the MFT database. So it is a relatively simple task for users familiar with Spotfire® or JasperReports® to create reports using the MFT database input.

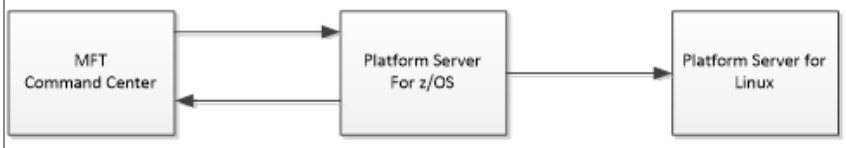
Sample Transfer Flows

Here are some sample transfer flows.





Flow 3: Command Center Initiates a Platform Server Transfer



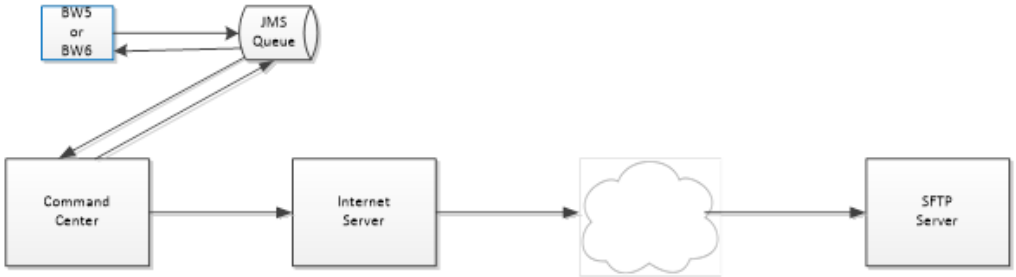
Command Center creates server definition for Platform Server for z/OS
Command Center initiates connection to Platform Server for z/OS
Command Center notifies Platform Server for z/OS to send a file to Platform Server for Linux
Command Center waits for a completion response from Platform Server for z/OS

Platform Server for z/OS receives request from Command Center
If Command Center is not waiting for transfer completion, Platform Server for z/OS notifies Command Center that the that request is accepted
Platform Server for z/OS initiates transfer to Platform Server for Linux
If Command Center is not waiting for transfer completion, when transfer completes, Platform Server for z/OS notifies Command Center that the transfer is completed

Platform Server for Linux processes the request like any other transfer request.

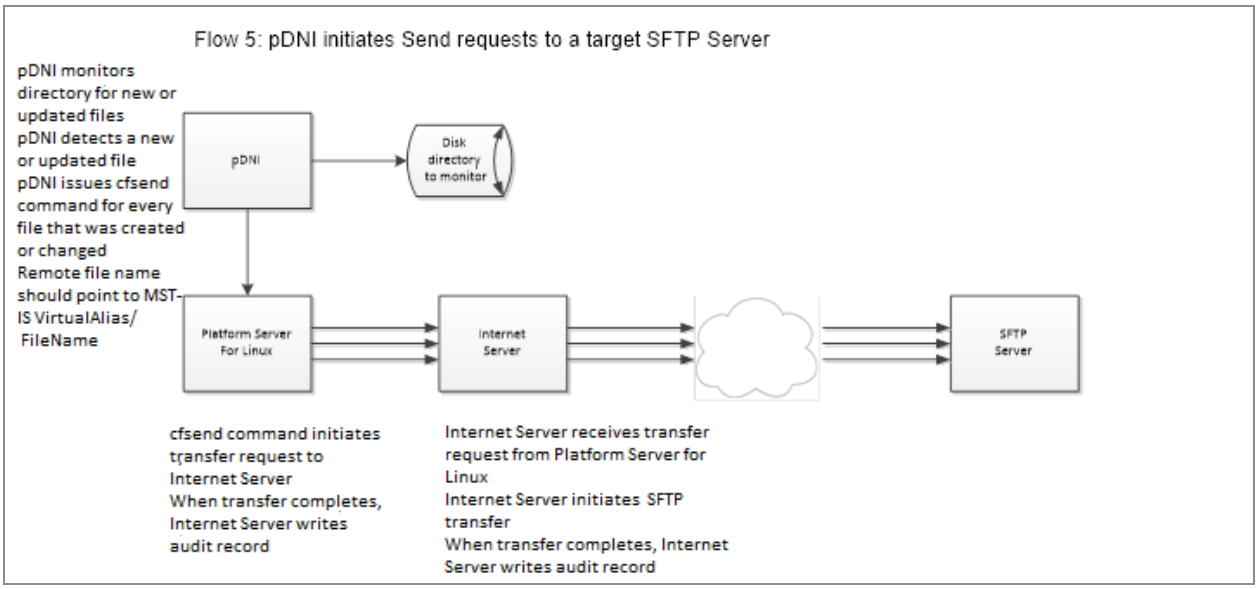
Flow 4: JMS initiates an Internet Server Transfer and waits for a response

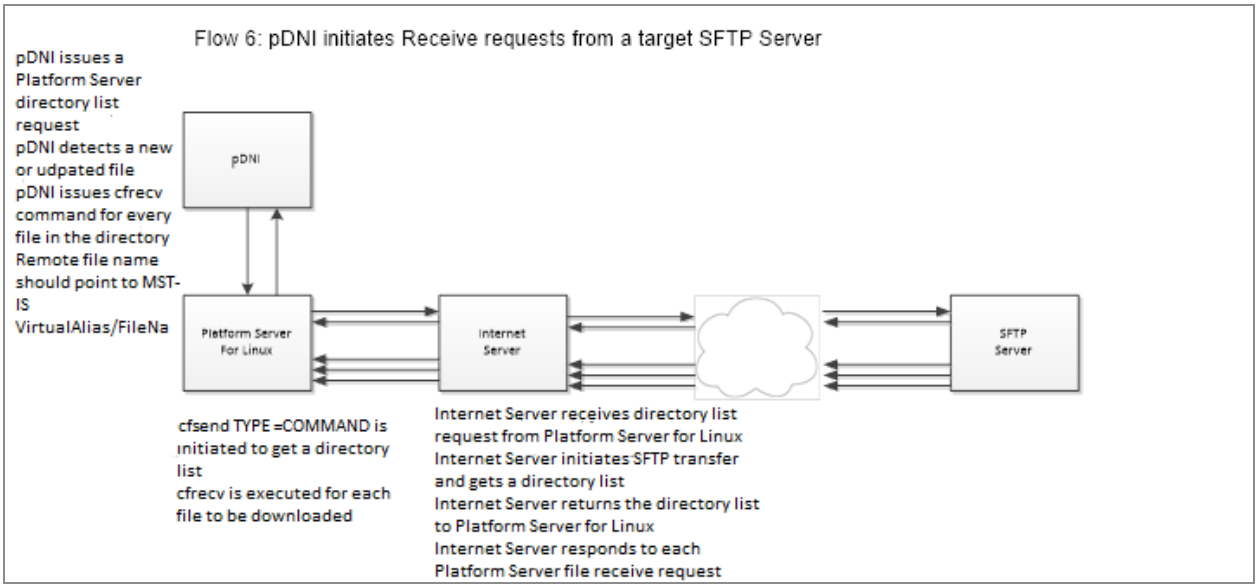
BW writes XML to JMS transfer queue
BW waits for "Transfer Submitted"message
BW waits for "Transfer Complete"message



Detects JMS message on the JMS transfer queue
Initiates transfer request to Internet Server
Writes "Transfer Submitted" message to JMS transfer queue
Polls the Audit file until the transfer completes
Writes "Transfer Complete" message to JMS transfer queue

Internet Server receives Command Center transfer request
Internet Server initiates transfer request to the target SFTP Server
Internet Server writes an audit record when the transfer completes


Flow 5: pDNI initiates Send requests to a target SFTP Server
pDNI monitors directory for new or updated files
pDNI detects a new or updated file
pDNI issues cfsend command for every file that was created or changed
Remote file name should point to MST-IS VirtualAlias/ FileName
pDNI
Disk directory to monitor
Platform Server For Linux
Internet Server
SFTP Server
cfsend command initiates transfer request to Internet Server
When transfer completes, Internet Server writes audit record
Internet Server receives transfer request from Platform Server for Linux
Internet Server initiates SFTP transfer
When transfer completes, Internet Server writes audit record


Flow 6: pDNI initiates Receive requests from a target SFTP Server
pDNI issues a Platform Server directory list request
pDNI detects a new or udpated file
pDNI issues cfrecv command for every file in the directory
Remote file name should point to MST-IS VirtualAlias/FileNa
pDNI
Platform Server For Linux
Internet Server
SFTP Server
cfsend TYPE =COMMAND is initiated to get a directory list
cfrecv is executed for each file to be downloaded
Internet Server receives directory list request from Platform Server for Linux
Internet Server initiates SFTP transfer and gets a directory list
Internet Server returns the directory list to Platform Server for Linux
Internet Server responds to each Platform Server file receive request

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 Internet Server is available on the TIBCO® Managed File Transfer Internet Server Product Documentation page.

- TIBCO® Managed File Transfer Internet Server *Managed File Transfer Overview*
- TIBCO® Managed File Transfer Internet Server *Installation*
- TIBCO® Managed File Transfer Internet Server *Quick Start Guide*
- TIBCO® Managed File Transfer Internet Server *User's Guide*
- TIBCO® Managed File Transfer Internet Server *Utilities Guide*
- TIBCO® Managed File Transfer Internet Server *API Guide*
- TIBCO® Managed File Transfer Internet Server *Transfer and File Share Clients User's Guide*
- TIBCO® Managed File Transfer Internet Server *Desktop Client User's Guide*
- TIBCO® Managed File Transfer Internet Server *Security Guide*
- TIBCO® Managed File Transfer Internet Server *Container Deployment*
- TIBCO® Managed File Transfer Internet Server *Release Notes*

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, and Slingshot 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 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 © 2003-2022. TIBCO Software Inc. All Rights Reserved.