TIBCO MFT Internet Server

Quick Start Guide

Software Release 7.2.6
September 2016

Two-Second Advantage®

TIBCO™

Important Information

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 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.

TIBCO, The Power of Now, TIBCO Managed File Transfer, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, TIBCO Managed File Transfer Platform Server, TIBCO Managed File Transfer Platform Server Agent, Edge Server, RocketStream Accelerator, and Slingshot are either registered trademarks or trademarks of TIBCO Software Inc. or its subsidiaries in the United States and/or other countries.

EJB, Java EE, J2EE, and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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.

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.

TIBCO® Managed File Transfer Internet Server with RocketStream® Accelerator is entitled TIBCO® Managed File Transfer Internet Server in certain other product documentation and in user interfaces of the product.

TIBCO welcomes your comments on this publication. Please address your comments to:

TIBCO Software Inc.
200 Garden City Plaza
Garden City, New York 11530 USA
Web site: http://www.tibco.com
Technical Support E-mail: support@tibco.com
Technical Support Call Centers:
North and South America: +1.650.846.5724 or +1.877.724.8227 (1.877.724.TACS)
EMEA (Europe, Middle East, Africa): +44 (0) 870.909.3893
Australia: +61.2.4379.9318 or 1.800.184.226
Asia: +61 2 4379 9318

When you send information to TIBCO, you grant TIBCO a non-exclusive right to use or distribute the information in any way TIBCO believes appropriate without incurring any obligation to you.

Table of Contents

Getting Started with MFT Internet Server

This guide has been developed to walk you through the steps necessary to configure the MFT Internet Server for the first time. A brief description of the steps necessary to get the Internet Server up and running is provided. It will be noted when a function or feature is specific to a single product.

This guide explains:

Once MFT Internet Server is installed, it is time to access the Internet Server screens.
The MFT Internet Server is accessed using the following URL:

https://[DNS_HostName]:[httpsPort]/cfcc/control?view=view/admin/start.jsp

When you are prompted for a userid/password you must log in with the Administrator credentials of **admin/changeit**.

Note: The admin password is now set to "changeit" at installation. This is for new installs only. In addition, passwords for all of the other pre-defined users MUST be changed by the admin before they can be used.

1 Applying the MFT Internet Server License Key

When MFT Internet Server is first installed, a temporary key is automatically installed and will expire 60 days from the first time the product is used.

To obtain permanent license keys login to download.tibco.com with your login id and password. If you do not have a login userid and password contact your TIBCO account representative.

To apply a new key navigate to **Administration > License > Add License Key** and enter the appropriate Server Name, Server Type, and License Key information in the fields provided:

- Server Name: Type in the Server Host Name used during the install. This can be found on the **Administration > License > Host Information** web page.
- Server Type: Select the Server Type **Internet Server**.
- License Key: Paste in the license key in the field provided. Note: Be careful not to copy any additional blank spaces on the end of a license key.

Once the fields are filled in, click the Apply button. Do this for each license you are applying.

If both Command Center and Internet Server are installed and sharing a database both license keys can be applied from the Command Center Administrator, Add License Key web page. To obtain the Host Name information for the Internet Server, navigate to the **Reports > Diagnostics** web page and expand the Internet Server diagnostics information. The server name will be displayed in the “License Keys” section.

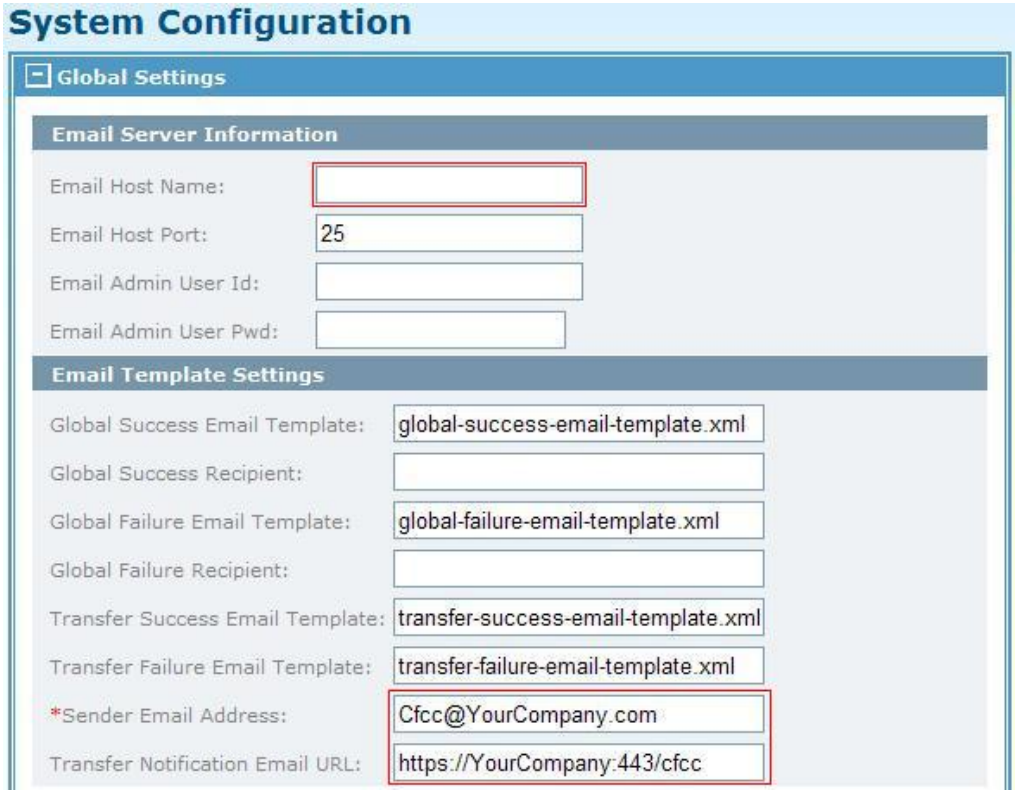
▲Back to Top

2 Adding your Email Server to MFT

There are some minimum MFT configurations we recommend being set. Adding your email server information is one of them.

2.1 Configure your Email Server Information

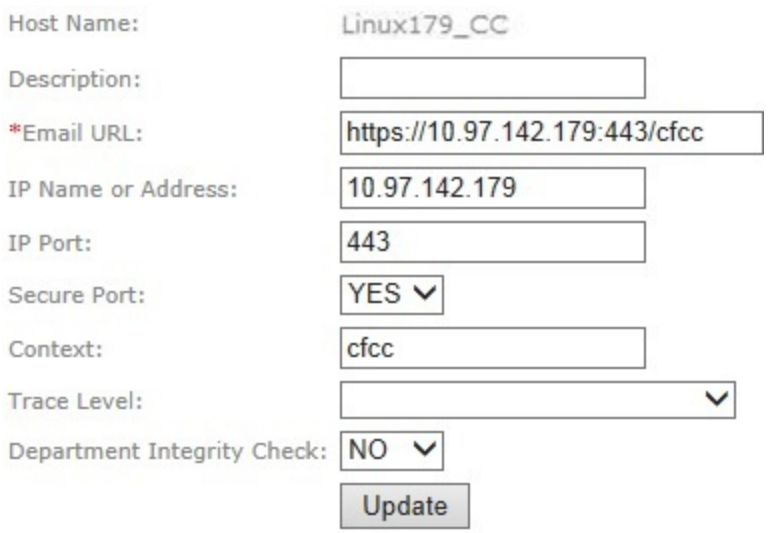
The first thing we recommend you configure is the IP or Host Name and port of your email server in order to receive various email notifications from many of the MFT features that can be configured with an email address(s). To do this navigate to **Administration > System Configurations** and expand the Global Settings window by clicking on the plus sign contained in the box next to the words "Global Settings" and you will see at the top of the web page the following email fields to be configured:



Fill in the **Email Host Name** with the IP or host name for the email server, the **Sender Email Address** that will be used on all emails sent from MFT Internet Server, and the **Transfer Notification Email URL** with the MFT Internet Server's IP, Host Name, or DNS name which will be used in email messages URL references when a Transfer Notification email is sent. By default port number 25 has been defined for your email server; if your server is using a different port number simply change the value to the correct port being used. Click the Update button when you have finished.

2.2 Configure Administrator Email URLs

Once you have configured your email server information above you will now want to expand the Local Settings section on the System Configurations web page. You will see your local MFT server settings as shown in the example below:



In this section set the Email URL with the MFT Internet Server IP, Host Name, or DNS name which will be used in email message URL references when an email is sent. If you are working in an environment with multiple Command Centers/Internet Servers This may be the address on one of these other servers defined in this field. It does not have to be the local servers address.

▲Back to Top

3 Adding Users

In order for users to be able to use MFT Internet Server to transfer files, their User Ids must be added to the MFT Internet Server database. The administrative user must have the AdministratorRight or UpdateTransferUserRight in order to add a User.

Part of the MFT Internet Server installation process adds 5 “Template Users” automatically to the database. By clicking on the **Add From Existing User** link a listing of those pre-existing users will be displayed. Simply click on one of the User Ids to copy the pre-existing user’s definition to a new user definition. The new user definition will have the same **Available Rights** and contain the same **Optional User Properties** of the User Id that was selected. The only thing left to do is to create a unique User Id, add the user’s Full Name, and create a Password for him/her. Click Add when you are finished to have the new user added to the database. You may edit any of the pre-existing user definitions before clicking on the Add button if you wish. As new user definitions are added more template user definitions are available to choose from.

3.1 Adding User Account

Transfer users are MFT Internet Server client end-users who access MFT Internet Server from the web-based file transfer client screens. From the main menu, select **Users > Add User**.

3.1.1 Required Parameters

1. Insert a **User ID** that will be used to login to MFT Internet Server/Command Center. The value cannot exceed 64 characters.
2. **Full Name** is used for the first and last name of the person on the account. The value cannot exceed 256 characters.
3. Insert a **Password** for the user to access MFT Internet Server/Command Center and then type the same password in the **Confirm Password** box. The value cannot exceed 32 characters.
4. **Expiration Date** that this user’s ID is no longer valid. MFT Internet Server defaults to one year from the current date.
5. **Valid Days** choose which days of the week this user is able to log on to access the system. Make certain that Administrative accounts have adequate access.
6. **Valid Start and End Time** define the period of time during a day that the user is able to log on to access the system. The default timeframe is a 24-hour period of access.
7. Assigned Rights. When adding a user, the screen sets the default right to “TransferRight”. Setting this right gives the user authorization to transfer files within the MFT Internet Server. If you want to authorize the user to initiate MFT Platform transfer requests, you must assign “FTTransferRight” to the user. By default the trial license will allow 50 Transfer Users and 50 OnDemand Transfer Users.

3.1.2 Optional Parameters

1. **Department** is the department to which this user belongs. This would only be used with Delegated Administration.
2. **Visibility** defines the level of accessibility that other departments have to this user and applies only when using Delegated Administration. The default is private.
3. **Description** of the user.
4. **Company Name** the user works for.
5. **Phone Number** of the transfer user.
6. **Start Date / End Date** specifies the starting and ending dates during which this user ID is valid, and can access the system.
7. **Client Protocol Allowed** indicates the type of protocols which will be allowed for this user while performing this transfer.

8. **Disable User** will disable a transfer users account which will cause them to fail to login to the system. If they are already logged in when this is enabled they will not be able to conduct a file transfer.
9. **LDAP Status** defines if and LDAP managed transfer user account is Active or not.
10. **Trace Level** would normally be turned on at the request of Technical Support in order to troubleshoot a problem. Leave at “No Tracing” during normal operation.
11. **Certificate DN** is used to define a transfer user’s certificate DN when conducting SFTP and SSH transfers using certificate authentication.
12. **Lock User** will lock a users account
13. **Can Change Own Password** sets whether a user can change their password.
14. **Password Never Expires** for the transfer user. If the Global Password Rules are in effect this setting will override these.
15. **Change Password at Next Login** will set the transfer users account to force a password change the next time they login.
16. **Email Address** is the user’s email address where MFT Internet Server will send notification when a file is available to be processed.
17. **Restrict User** causes this transfer user to be restricted to an IP and/or Netmask to connect.
18. **IP Address or IP Name** is the IP or Host Name the transfer user is restricted to using to connect to the system.
19. **Netmask** is the Netmask the transfer user is restricted to be using when connecting to the system.

3.1.3 PGP Information

1. **Allow User to Add PGP Key** can be set to allow a transfer user using PGP keys to load their PGP Key to the system through the This Client.

3.2 Manage Users

To modify a particular User’s information select **Users > Manage Users**. This displays the first 100 users defined. It also displays an expandable box that allows you to enter Selection Criteria for the user (or users) that you wish to modify. When you have found the user that you want to modify, click on the “User Id”. This will display the detailed information for that user, when the modification is complete, press the “Update” button to save the modification.

▲Back to Top

4 Adding Server Definitions

Server Definitions contain the information that MFT Internet Server/Command Center needs to communicate with the following server types: MFT Platform Server, FTP, Local servers, SSH and AS2. The Server definition defines how the supported clients can gain access to a file.

Many different Server definitions can be configured within a single MFT Internet Server system. MFT Internet Server supports five types of Server Definitions. The servers that you define depend on the product that is installed as well as the location of the files needed for file transfer requests. The five Server Types are:

1. **Platform Server –** This definition allows Internet Server File Transfer Clients to access files located on an MFT Platform Server. It also allows MFT Internet Server to manage and initiate transfers on MFT Platform Servers.
2. **FTP Server** - This is used by the MFT Internet Server. This allows Internet Server File Transfer Clients to access files located on an FTP server.
3. **Local Server -** This is used by the MFT Internet Server. It allows Internet Server File Transfer Clients to access files located on the MFT Internet Server.
4. **SSH Server -** Allows file transfer clients to access files located on an SSH server.
5. **AS2 Server** - Allows file transfer clients to access files located on an AS2 server.

4.1 Adding a Server Definition

From the main menu choose **Servers > Add Server**

4.1.1 Required Parameters

1. Type the **Server Name** for the proxy server. The value cannot exceed 32 characters.
2. **Host Name or IP Address** of this server. Maximum value is 80 characters.
3. **IP Port** defines the IP Port of the remote server.
4. The **Server Type** defines the Server Type that MFT Internet Server/Command Center will be communicating with. *Note: For adding an SSH server type see section 4.1.3 Adding an SSH Server Definition for additional information.*
5. The **Server Platform** defines the type of platform where the Server is executing. The four platforms supported are UNIX, WINDOWS, z/OS and IBM I, UNISYS2200.

4.1.2 Optional Parameters

Expandable boxes define optional Server Definition parameters.

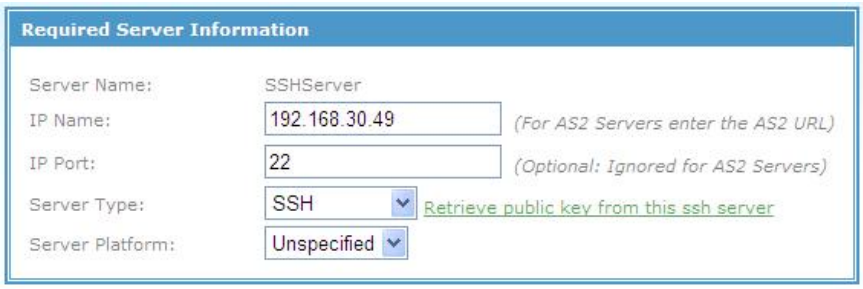
1. **Platform Server Options**: Contains default Encryption parameters. This setting is only valid when Server Type is Platform Server.
2. **FTP Options**: Defines FTP properties including case sensitivity, connection type, and SSL options. This setting is only valid when Server Type is FTP.
3. **SSH Options**: Allows the selection of an SSH key used for authentication to the SSH Server. This setting is only valid when Server Type is SSH.
4. **AS2 Options**: Define server options that are only used when Server Type is AS2.
5. **Local Options**: Allows a Server File Name prefix to be defined. This is used only when Server Type is LOCAL. It defines the directory that is prefixed to the Server File Name defined on the Transfer definition. This allows you to restrict users to access particular directories.
6. **Server Credentials**: Allows you to define the default Userid and Password for a MFT Platform server, SSH server and FTP Server.
7. **Additional Server Properties**: Allows you to define miscellaneous Server definition fields. The Server File Name Prefix is used only when the Server Type is Local. It defines the directory that is the starting point for all Internet Server transfers.

8. **Platform Server Collector Options**: Defines Server options that are used only when the Server Type is defined as Platform Server and the MFT Platform Server should be managed by the MFT Internet Server.
9. **PGP Information**: Defines PGP specific information for this server.

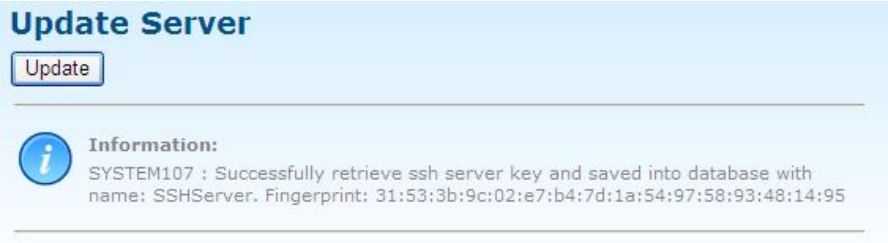
4.1.3 Adding an SSH Server Definition

When you add an SSH server definition to MFT Internet Server you must retrieve the SSH server's public key. To do this, follow the instructions below:

1) Navigate to Servers>Manage Servers and click on the link to the SSH server you added earlier with *Server Credentials* defined in order to log on to the remote SSH server.
2) Notice the *Required Server Information* section now contains the link Retrieve public key from this ssh server:



3) Click on the Retrieve public key from this ssh server link and the remote SSH servers public key will be pulled into the MFT database and you will see something like this:



6) Click on the Update button to complete the SSH server definition.

4.2 Manage Servers

To modify a particular Server Definition select:
Servers > Manage Servers
This displays all the Server definitions defined to MFT. It also displays an expandable box that allows you to enter Selection Criteria for the Server (or Servers) that you wish to modify. When you have found the Server that you want to modify, click on the "Server Name". This will display the detailed information for that Server definition, when the modification is complete, press the "Update" button to save the modifications to the Server definition.

▲Back to Top

5 Adding Transfer Definitions

MFT Internet Server versatility includes a variety of file transfer options, from post-processing to modifying the file on the remote end (Write Mode). For basic file transfers, you are required to complete the required information section. For advanced file transfer options please refer to the MFT Internet Server manual.

5.1 Adding a Transfer Definition

From the main menu choose **Transfers > Add Transfer**

5.1.1 Required Parameters

1. **Client File Name** is the full path name of the file on the client machine. This is a suggested value that can be updated by the client when they initiate the transfer request.
2. **Server File Name** is the full path name of the file on the Server. Remember that the server could be the MFT Internet server, an FTP server, an SSH server, an AS2 server, or an MFT Platform server, depending on the Server Name associated with the transfer definition.
3. **Directory Transfer** means that the user is able to transfer the contents of an entire directory – a transfer user has the ability to specify a directory and transfer all files and subdirectories from within the directory, at once.
4. **Description** is a brief description of the file.
5. Select the **Authorized User ID** or the **Authorized Group ID** which will be allowed to access this file.
6. **Server Name** defines the server associated with this transfer
7. **Transfer direction** is either **Upload** to the Server or **Download** to the Client or **Both** (Setting **Both** will generate two transfer definitions. One used for uploads and one for downloads.)
8. **Client Protocols Allowed**. Select the protocol that is allowed for this transfer. The default is ALL.
9. **Department**. Used with Delegated Administration.
10. **Virtual Alias** is a mapping to the Server File Name specified in the transfer definition. This alias is used when the client is FTP, SSH, or MFT Platform Server.

5.1.2 Optional Parameters

Expandable boxes define optional Server Definition parameters.

1. **Server Properties** allows you to define default credentials for the server as well as default Encryption (if supported)
2. **Additional Transfer Properties** allows you to define Transfer Descriptions, Data Properties, Accessibility, Checkpoint Restart and Diagnostic information. One of the more important fields is the **Write Mode**. The **Write Mode** allows you to define rules to determine if the file can be written to the server. For example, a **Write Mode** of **Create** will allow a transfer to complete only if the file does not exist on the server. Note that this parameter is for Uploads only. For a download, the **Write Mode** of **CreateReplace** is always used.
3. **Email Notification** allows you to send emails when a Transfer definition is created, or when a file transfer completes, either successfully or unsuccessfully.
4. **Post Processing Actions** allows you to perform actions when a transfer completes.
5. **z/OS and UNIX Properties** allows you to define platform specific information. This setting is only valid if the Server Name is an MFT Platform Server.
6. **PGP Information** defines the PGP Information that can be associated with a Transfer.

7. **Client Permissions** define additional actions that can be taken by the FTP, SSH, and Desktop .NET clients. These include, Delete, Rename, Create Directory, Remove Directory and Client Transfer Mode.

5.2 Managing Transfers

To modify a particular Transfer record select:
Transfers > Manage Transfers
This displays the first 100 transfers defined. It also displays an expandable box that allows you to enter Selection Criteria for the transfer (or transfers) that you wish to modify. Within the Selection Criteria box, it allows you to “List transfers by users”. This will display a screen of valid users. When you select a user from this screen, all transfer definitions for this user are displayed. When you have found the transfer that you want to modify, click on the “Transfer Id”. This will display the detailed information for that transfer, when the modification is complete, press the “Update” button to save the changes.

▲Back to Top

6 Setting up MFT Platform Server Transfers

Step 1: MFT Platform Server Configurations

Navigate to **Administration > Transfer Servers > Platform Server > Configure Platform Server**. Expand the Platform Server Settings windows for your MFT Platform server. Configure the server as instructed in section *Platform Server: Configure Platform Server* in the MFT Internet Server User Guide. The IP Port needs to match the Port Number used in the MFT Platform Server transfer. This port is only used between MFT Internet Server and MFT Platform Server.

Step 2: Start the Platform Server

Navigate to **Administration > Transfer Servers > Platform Server > Platform Server Status**. Click the **Start Server** button.

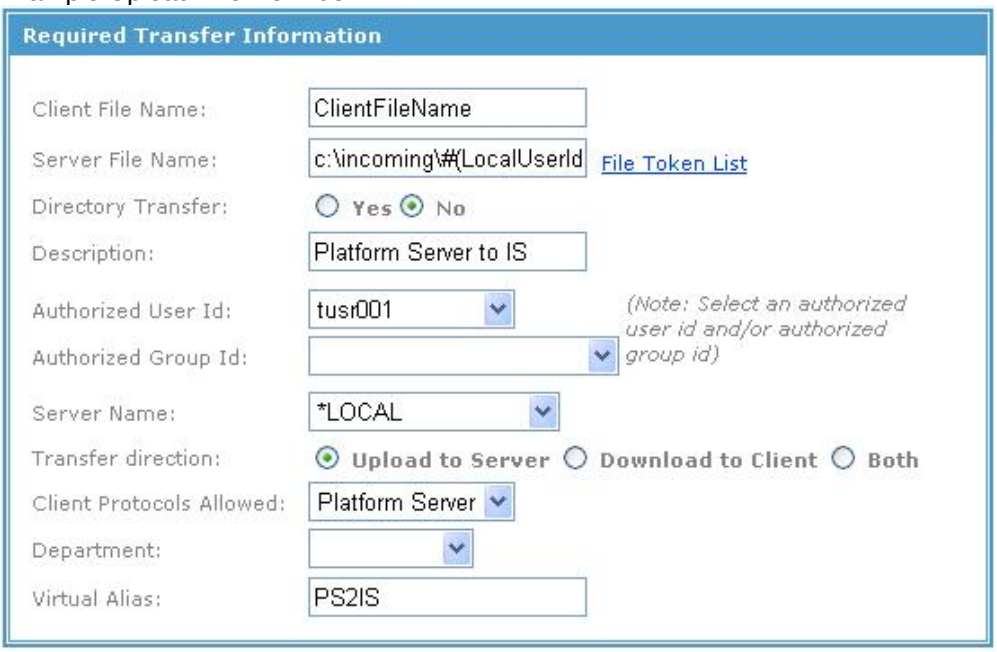
Step 3: Create an Upload and Download File Definition

Step 3.a Uploading a file from MFT Platform Server for Windows to MFT Internet Server:

In order for MFT to accept a file transfer from a MFT Platform Server, you need to create an upload file definition. Navigate to **Transfers > Add Transfer** and fill in the *Required Transfer Information* section with the information below:

1) **Client File Name**: This can be anything. Use a place holder (such as *). The file selected by the client will replace the value specified here.
2) **Server File Name**: Set the path and file name for the files that will be written. We suggest you add to your Server File Name path the date and time File tokens to your request. This will help differentiate the files as they come in.
3) **Directory Transfer**: Select No. (Could be set to Yes, but our example sends a single file.)
4) **Description**: Add a short description.
5) **Authorized User Id**: Choose the user id from the drop down lists that will be used to make this file transfer.
6) **Server Name**: This can be set to any server. This is set to *LOCAL for this example.
7) **Transfer Direction**: Select Upload to Server.
8) **Client Protocols Allowed**: Set to Platform Server.
1) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.
2) **Virtual Alias**: Add the alias that the MFT Platform Server user will use for transfers.
3) When you are done click on the Add button.

Example Upload File Definition

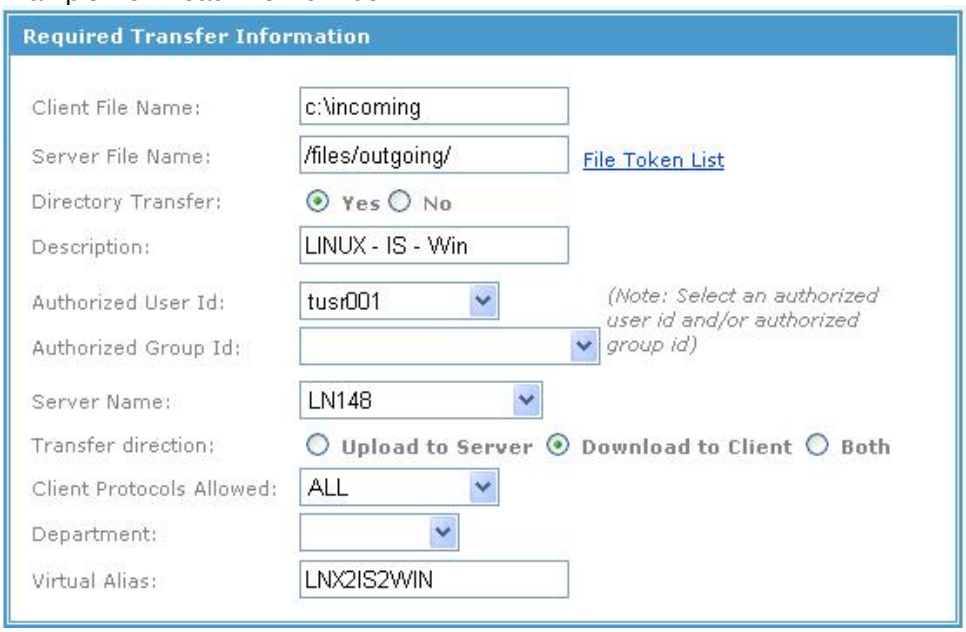


Step 3.b Downloading a file from MFT Internet Server to MFT Platform Server:

You can download files from MFT Internet Server with MFT Platform Server as well as upload files. To do this you need to create a download file definition. For our example we will configure a directory download from a LINUX server that has MFT Platform Server for UNIX installed to download files using MFT Platform Server for Windows via MFT. Navigate to **Transfers > Add Transfer** and fill in the *Required Transfer Information* section with the information below:

1) **Client File Name**: This can be anything. Use a place holder (such as *). The file selected by the client will replace the value specified here.
2) **Server File Name**: Directory where all the files to be downloaded are located on the server.
3) **Directory Transfer**: Select Yes.
4) **Description**: Add a short description.
5) **Authorized User Id**: Choose the user id from the drop down lists that will be used to make this file transfer.
6) **Server Name**: Server containing the files that will be downloaded.
7) **Transfer Direction**: Select Download to Client.
8) **Client Protocols Allowed**: Set to Platform Server.
9) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.
10) **Virtual Alias**: Add the alias that the MFT Platform Server user will use for transfers.
11) When you are done click on the Add button.

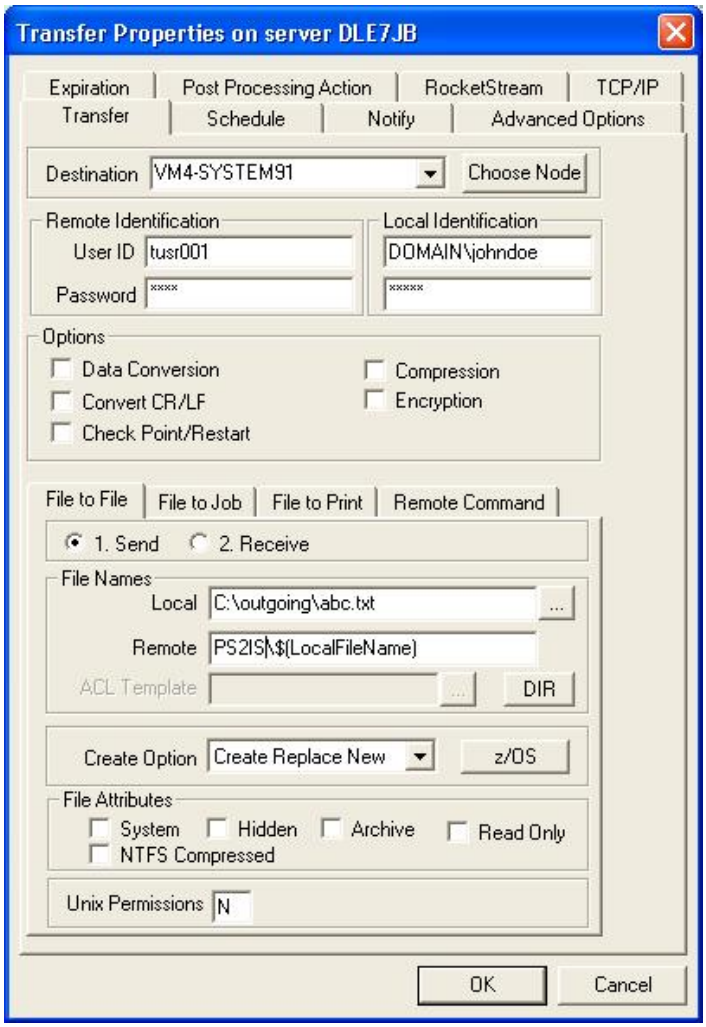
Example Download File Definition



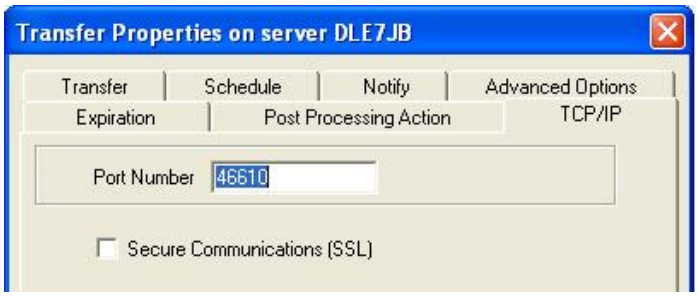
Step 4: Configuring MFT Transfer Templates to upload and download files

Step 4.a MFT Platform Server for Windows Transfer template to upload files to MFT Internet Server:

The MFT Platform Server user must configure a Transfer template in order to upload a file to MFT Internet Server. Below is a screen shot of a Transfer template from MFT Platform Server for Windows that coincides with our MFT Internet Sever file definition we configured above in Step 3.a, notice the key fields **Destination** (MFT Internet Server), **User ID** (MFT's User Id), and **Remote File Name** (MFT's Virtual Alias in Upload File Definition):



The user must make sure they have the port defined that MFT Platform Server is listening on the one configure in Step 1. This would be located on the TCP/IP tab for the Transfer template:

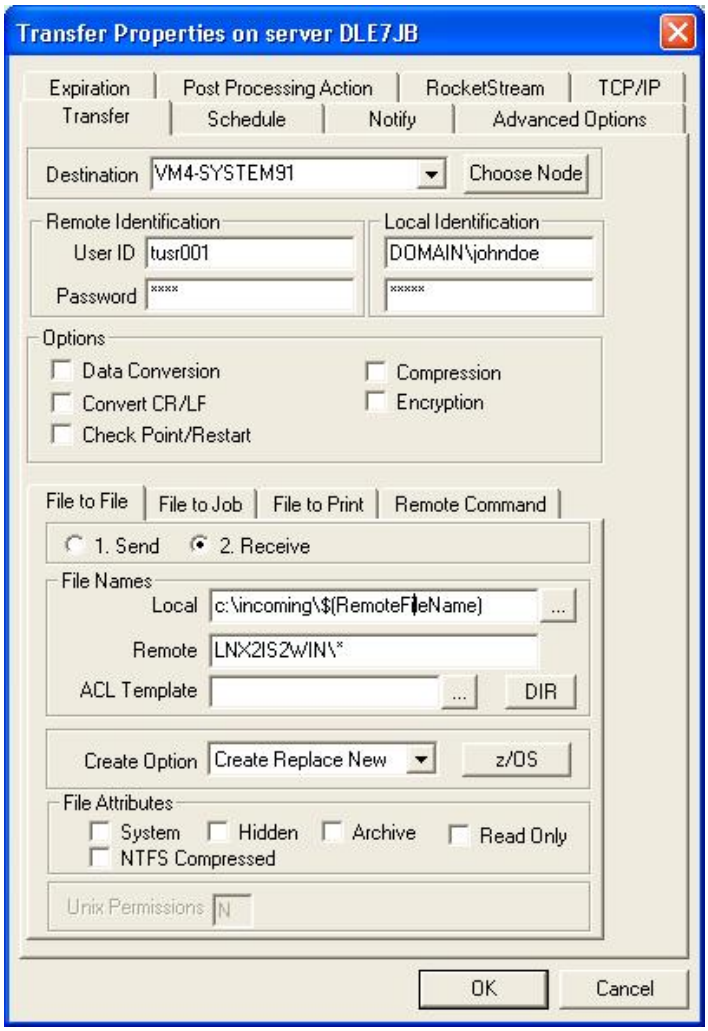


Once the Transfer panel is complete the user would click on the Ok button.

The information entered in the MFT Platform Server Transfer panel will go to MFT Internet Sever (based on the Destination and Port Number) and pick up the file transfer definition based on the Virtual Alias information used. Then the MFT Internet Server will send the transfer to the proper remote system based on the Server Name defined. In our case we had the file upload to *LOCAL which is the MFT Internet Server.

Step 4.a MFT Platform Server for Windows Transfer template to download files from MFT:

Now the MFT Platform Server user must configure a Transfer template to download files that will be coming from the remote LINUX server through MFT Internet Server. Below is a screen shot of a Transfer template from MFT Platform Server for Windows that coincides with our MFT Internet Server file definition we configured above in Step 3.b, notice the key fields **Destination** (MFT Internet Server), **User ID** (MFT's User Id), **Local File Names** (use file name tokens), and **Remote File Name** (MFT's Virtual Alias in Upload File Definition):



We suggest you add to your **Local File Name** path the date and time File Tokens for MFT Platform Servers to your request. This will help differentiate the files as they come in.

Notice in the **Remote File Name** field we used the asterisk (*) wild card after the Virtual Alias name that was defined in our download file definition we setup in Step 3b. This will allow all the files contained in the Remote LINUX server's directory to be sent to the MFT Platform Sever on Windows.

▲Back to Top

7 Setting up PGP Transfers

Uploading a Single PGP Encrypted File to MFT

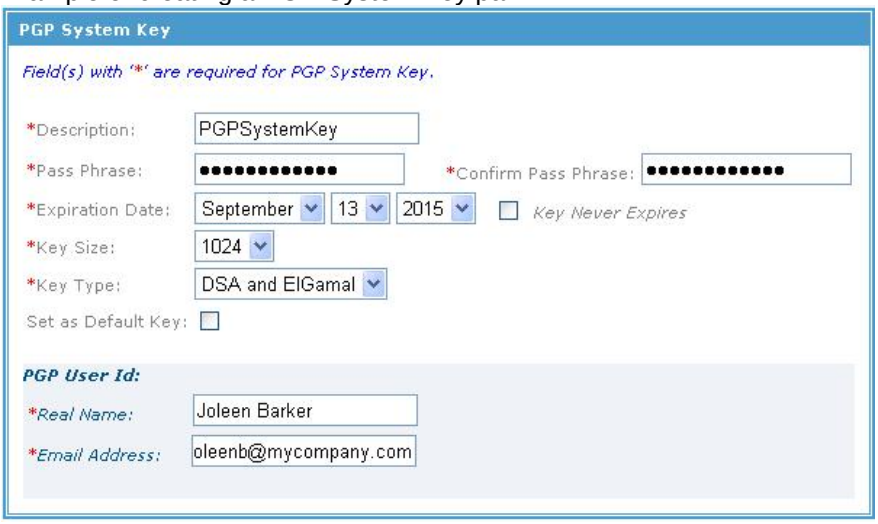
Step 1: Add a PGP System Key to MFT

Before we can do anything we must first give MFT Internet Server a PGP System Key. You can create a key pair through the MFT Internet Server or follow your PGP or GPG program instructions to generate a set of keys and then put them in ASCII Armored format. The MFT PGP System key will consist of both a PGP Secret key and a PGP Public Key. The Public Key will be used by the users making the transfers. The secret key remains secret and is not meant to be shared. *Note – The first PGP System Key created will be set as the Default Key.*

Create a PGP key pair by navigating to **Administration > Keys > PGP System Keys > Create PGP Key** and following the instructions below.

1) Fill in all the requested data.
2) Click on the Create Key button when you have finished entering the data.

Example of creating a PGP System Key pair:



Step 2: Configuring the User for PGP transfers.

Next the transfer user conducting the transfer requests must be configured in MFT. If you need help creating a user id go to section *Add User* of the MFT Internet Server User Guide.

In order for the user to send a PGP encrypted file he/she will need the MFT PGP Public Key. This is what you added in Step 1. This will allow the user to encrypt files that will be uploaded to the MFT Internet Server. For the user to be able to get the MFT PGP Public Key the Admin has two options. The Admin can simply e-mail the user the MFT PGP Public Key for the user to add to his/her key ring or the user can log in to the file transfer Thin Client and click on the Keys icon which will display the MFT PGP Public Key for them to cut and paste into a file in order for them

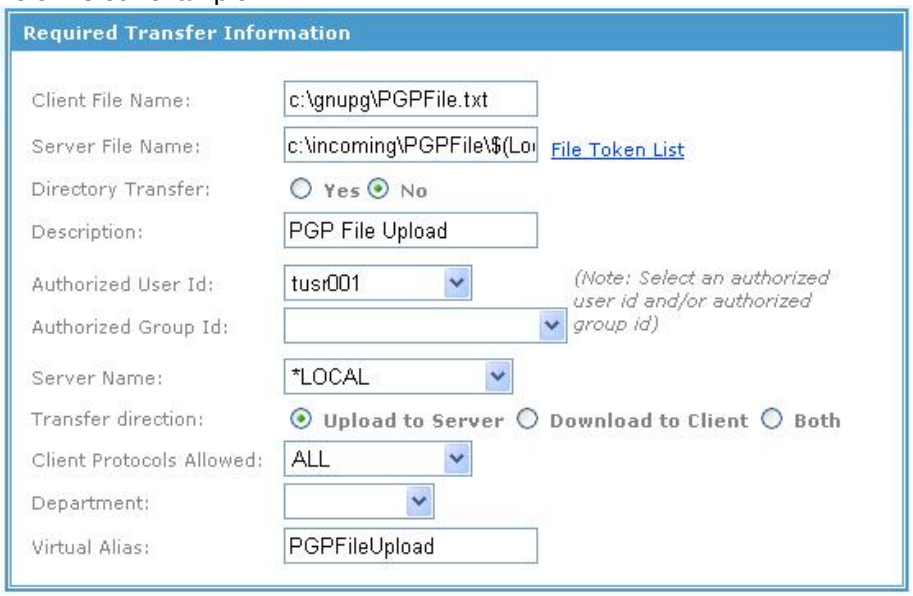
to import the key into their key ring. (Please see your program instructions in order to import and export PGP keys.) See example below:

Step 3: Set up the file transfer definition

You now need to setup a transfer definition to upload a single file for the user by navigating to **Transfers > Add Transfer**. Fill in the following fields as follows:

1) **Client File Name**: The path and file name of the PGP encrypted file that will be uploaded.
2) **Server File Name**: Set the path and file name for the file that will be written. We suggest you add to your Server File Name path the date and time File tokens to your request. This will help differentiate the files as they come in.
3) **Directory Transfer**: Set to No. (This could be set to Yes, but our example is sending a single file.)
4) **Description**: Add a short description users will see when they log into the Thin Client.
5) **Authorized User Id**: Set the user id that will be conducting this upload.
6) **Server Name**: Set this to *LOCAL for our example.
7) **Transfer Direction**: Select Upload to Server.
8) **Client Protocols Allowed**: Leave as ALL
9) **Virtual Alias**: If you will be using an FTP, SSH or MFT Platform Server Client to upload this file add an Alias.
10) Open the *PGP Information* section of the file transfer definition page.
11) Select **Decrypt** (if you do not enable this, the file transferred will be sitting in an encrypted state on the MFT Internet Server).
4) Click on the Add button when you are done.

Below is our example:



Now user tusr001 can transfer his encrypted file to the MFT Internet Server, where it will be decrypted by the MFT PGP Secret Key.

Note: If the user does not encrypt the file before transferring the following error will be reported in the Audit records:

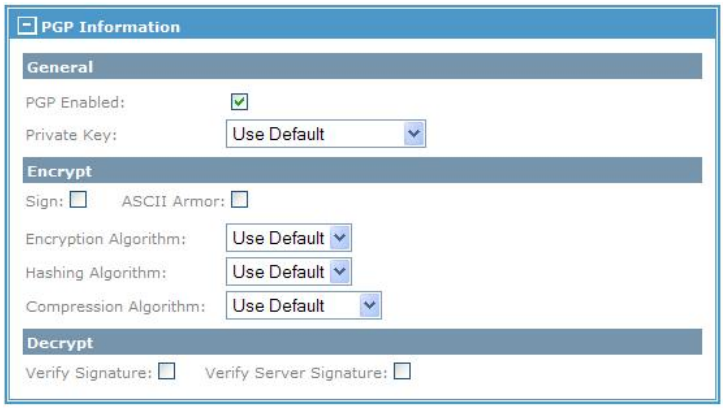
Exception: java.lang.Exception: Public PGP key for *LOCAL not found

Uploading a Text File to MFT Internet Server where it will be PGP Encrypted

Step 1: Add a PGP Server

When you want to encrypt a plain text file while it is being transferred up to a server you must configure a server to be a PGP server. Your server will have a PGP key pair. From that pair you will need the PGP Public Key in Base64 format.

First Navigate to **Servers > Add Server**. Fill in the Required Server Information section and then expand the PGP Server Information section. Here you will Select PGP Enabled. If this is box is selected all files going to this server will be PGP encrypted. If you want the file to be signed and left in an ASCII Armored format select these boxes as well. Click "add" when you are done. See our example below:



Step 2: Assign the PGP Server a PGP public Key to use

Now you have to assign a PGP Public Key to the PGP Server that you defined in Step 1. Navigate to **Administration > Keys > PGP Public Keys > Add PGP Key**.

1) Select **Server**.
2) Choose the Server from the drop down list
3) Select **Enabled**.
4) Add the PGP Public Key you have for the server.

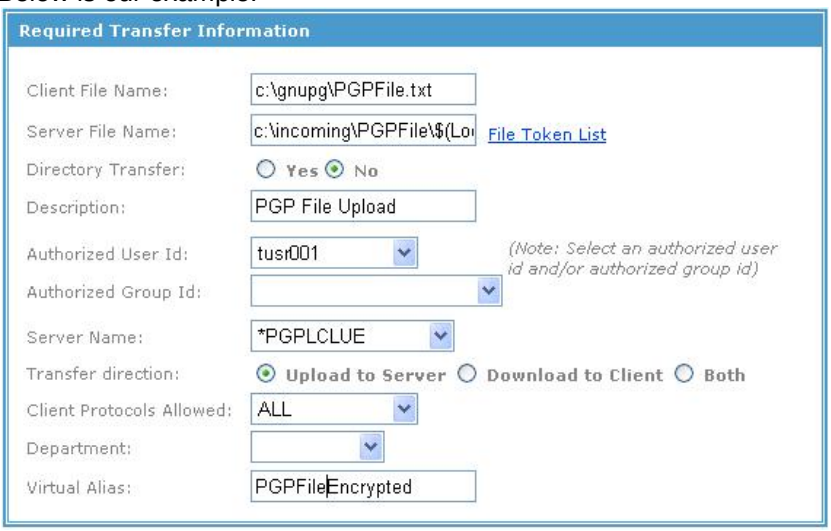
Step 3: Set up the file transfer definition

You now need to setup a transfer definition to upload the file. Navigate to **Transfers > Add Transfer**. Fill in the following fields as follows:

1) **Client File Name**: The path and file name of the text file that will be uploaded.
2) **Server File Name**: Set the path and file name for the file that will be written. We suggest you add to your Server File Name path the date and time File tokens to your request. This will help differentiate the files as they come in.

3) **Directory Transfer**: Set to No. (This could be set to Yes, but our example is sending a single file.)
4) **Description**: Add a short description users will see when they log into the Thin Client.
5) **Authorized User Id**: Set the user id that will be conducting this upload.
6) **Server Name**: Set this to PGP Server you configured in Step 1.
7) **Transfer Direction**: Select Upload to Server.
8) **Client Protocols Allowed**: Leave as ALL
9) **Virtual Alias**: If you will be using an FTP, SSH or MFT Platform Server Client to upload this file add an Alias.
10) Click on the Add button when you are done.

Below is our example:



Now when the user assigned to this file definition uploads his text file to the server it will be encrypted with the PGP Public key we defined in Step 2 to be decrypted at a later time.

Admin steps to follow when doing a proxy to a MFT Platform Server with a PGP encrypted file:

For this example I upload a PGP encrypted file from my windows PC to a LINUX system via MFT Internet Server which will decrypt the file on the LINUX system.

1) The Admin would have to add the LINUX Secret Key (this includes the Public Key as well) to the PGP System keys and enabled it.
2) Then the Admin would navigate to **Transfers > Add Transfer** and configure the upload to the LINUX server and in the PGP Information section configure the PGP Private Key to be set to the LINUX servers Secret Key.

On the transfer users machine would be a file that he/she encrypted with the LINUX Public Key. (The user would have had access to this public key prior to this in order to complete this step.) The user would log into the Thin Client and proceed to upload the file.

The file is then decrypted when it hits the MFT Internet Server using the LINUX Secret key that the Admin had configured earlier and then the file is sent to the LINUX system.

Admin steps to setup a single PGP encrypted file download:

1) Navigate to **Administration > Keys > PGP Public Keys > Add PGP Key** and add a PGP Public Key for the user that will be performing this transfer request.

2) Set up a file transfer definition to download a single file. (When setting up the Client File Name in the file transfer definition we suggest using a file extension the PGP software is familiar with to avoid errors. For example with GPG the software will be expecting an encrypted file with the extension .gpg before it can decrypt it correctly. The alternative to this is the user change the file name that is downloaded through the Thin Client.) In the PGP Information section of the file transfer definition check off Encrypt and leave all other settings to defaults.

The user would then log into the Thin Client and download the file(s). They will be sitting in the directory in which it was downloaded to in an encrypted state for the user to decrypt at a later time with his/her PGP secret key.

▲Back to Top

8 Setting up MFT SSH Server

MFT Internet Server provides an internal SSH server that can be configured and used to perform SSH transfers. Configuring this server allows MFT to become a host as opposed to adding an SSH server to the server definitions where we are then the client.

Note: Some SSH clients do not support zero byte file transfers and will error out.

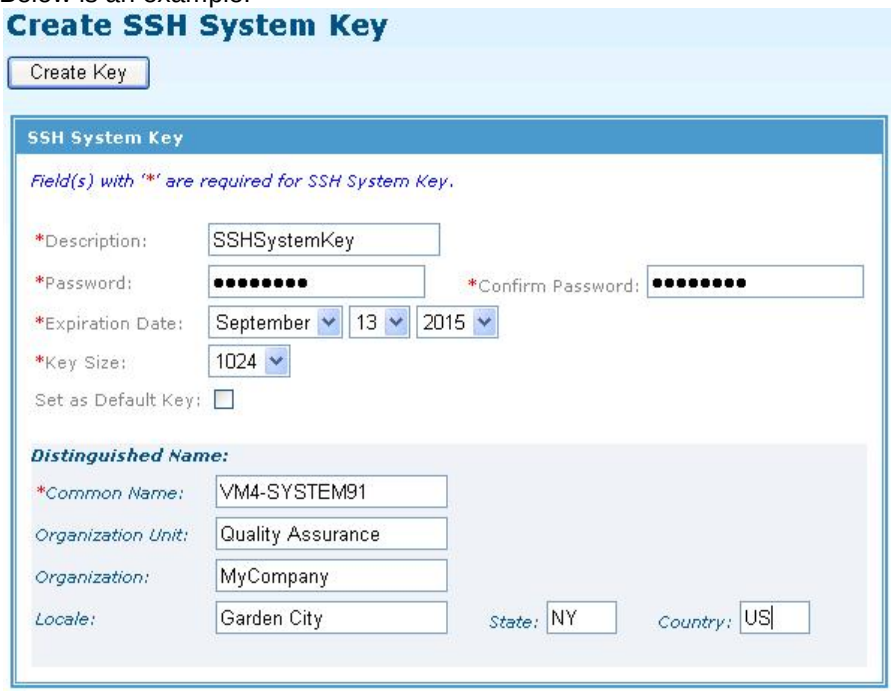
Step 1: Create an SSH System Key

All SSH servers have a Key/Certificate pair. MFT can create the key pair for you or you may import existing keys. For our example we will generate a new key pair for our MFT SSH Server to use as the default keys.

Navigate to **Administration > Keys > SSH System Keys > Create SSH Key**. Fill in the following fields to create your key:

1) **Description**: Give the key a descriptive name using this field.
2) **Password**: Give this key a password/pass phrase and confirm it.
3) You can accept the default **Expiration Date** and **Key Size** or edit them if you wish.
4) Check on the **Set as Default** box.
5) Add a **Common Name** under the *Distinguished Name* section.
6) Fill in the rest of the *Distinguished Name* section if desired.
7) Click on the Create Key button when you are done.

Below is an example:

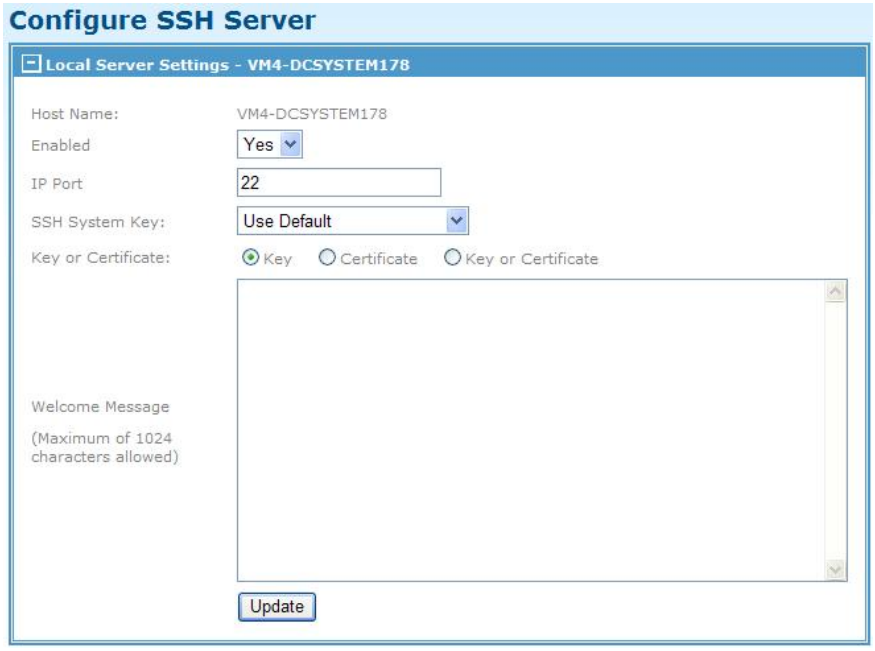


Step 2: MFT SSH Server Configurations

Navigate to **Administration > Transfer Servers > SSH Server > Configure SSH Server**. Expand the SSH Server Settings windows for your MFT SSH server. Configure the following:

1) By default the server is not enabled. Change the **Enabled** field to read **Yes**.
2) By default the **IP Port** is set to 22, change this port if desired.
3) By default the SSH System key will be the SSH System you created in the first step. You may enter more keys to the MFT System and you would choose the key pair you want to use by clicking on the appropriate one from the drop down menu. For our example we are using the default key.
4) (Optional) Add a Welcome Message that users can see when they connect to the server.
5) Click the Update button when you are done.

Below is an example:

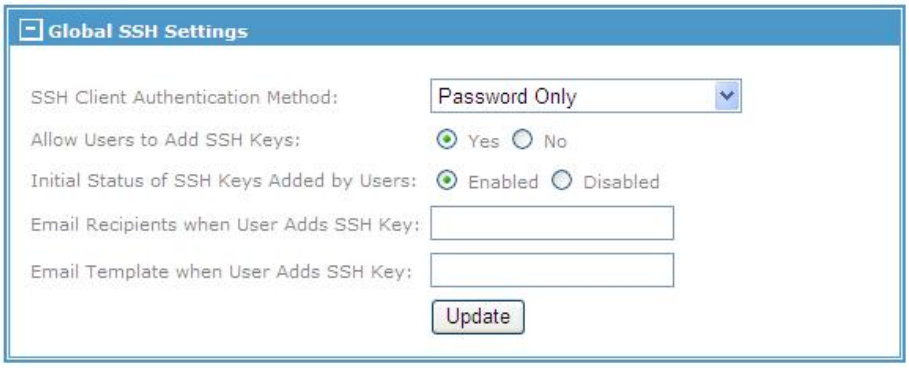


Step 3: Start the MFT SSH Server

Now that we have created our SSH System Key and configured our SSH server's settings we can start the server. Navigate to **Administration > Transfer Servers > SSH Server > SSH Server Status**. Click the **Start Server** button.

Step 4: Configure MFT SSH Server Authentication

By default MFT SSH Server is configured to perform *Password Only* authentication. Some environments may want to change this to *Key/Certificate Only* authentication or use both. Navigate to **Administration > System Configurations** and expand the Global SSH Settings windows and you should see the following:



Field	Description
SSH Client Authentication Method	Set the authentication method to be used for the MFT SSH server. Values: Password Only, Key/Certificate Only, Key/Certificate or Password, Key/Certificate and Password. See *SSH Key/Certificate Authentication* for more information on adding SSH public keys to the MFT database.
Allow Users to Add SSH Keys	If you want to allow a user to add their own SSH public keys to the MFT database set this to Yes.
Initial Status of SSH Keys Added by Users	When a user add their own SSH public key do you want that key to be enabled or disabled.
Email Recipients when User Adds SSH Key	Enter the email address(es) to be used for an email to be sent to when a user has added a new SSH Public Key to the MFT database. Separate multiple email addresses with a comma.
Email Template when User Adds SSH Key	The email template that will be used when sending out notification to the email recipient in the field above. The default email template can be found in the <WEB_Server>\cfcc\email-templates\email-ssh-key-notification-template.xml

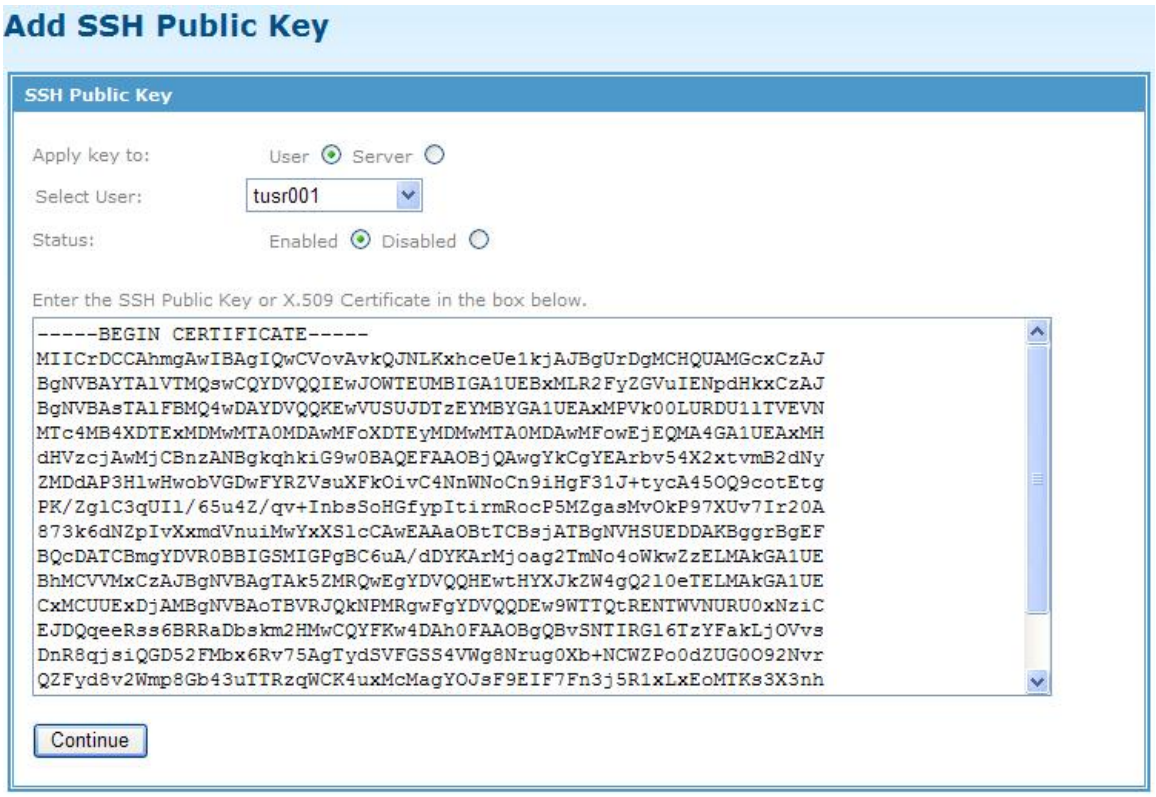
SSH Key/Certificate Authentication

Any SSH Client Authentication Method setting other then **Password Only** would require an SSH public key/certificate to be setup for either a user (client) who has been added to the MFT database or a particular server you may have defined in the server definitions configurations. In the example below we will configure a MFT user to associate with a particular SSH public key:

Adding an SSH Public Key to MFT Internet Server

Navigate to **Administration > Keys > SSH Public Keys > Add SSH Key**

1) Select **User**.
2) Choose the user from the drop down list
3) Select **Enabled**.
4) Copy and paste the SSH Public Key into the provided text box.
5) Click on the Continue button



6) Verify the key/certificate information and click on the Continue button again.

▲Back to Top

9 Example MFT FTP Server Transfer

These examples show the Client File Name, the Server File Name and the Virtual Alias parameters that are set in a transfer definition from MFT Internet Server and how they are resolved during an FTP transaction.

Let's assume that there is a directory called "c:\test1" (Client File Name) on the client's side containing files file1.txt and file2.txt. The client will perform an FTP Upload (put) and an FTP Download (get) to and from the MFT FTP Server on 192.168.222.222. There is a directory called "c:\test2" on the MFT Internet Server (Server File Name) that contains files file3.txt and file4.txt. The transfer will be done using a userid of "user1".

Two Transfer Definitions should be created for "user1" in order to perform these FTP transactions, one for Upload and one for Download. As stated earlier, both files should point to the same "c:\test2" directory on the Server side where the files will be transferred to and from. Also, this directory must be assigned the same Virtual Alias parameter value in both the Upload and the Download File Definitions. For this example, the Virtual Alias will be "/FtpFiles".

Step1.

User "user1" performs an FTP login from the client side "c:\test1" directory onto MFT FTP Server on 192.168.222.222. He will see the "Welcome!" message configured on the MFT Server.

```
C:\test1>ftp 192.168.222.222
Connected to 192.168.222.222.
220-TIBCI MFT FTP Server (v. 7.2.1)
220 This is the MFT Server 7.2.1 on 192.168.222.222 Welcome!
User (192.168.222.222:(none)): user1
331 Password required for user1
Password: ************
230 Logon OK. Proceed.
```

Step 2.

User "user1" is able to see the list of files available for the Upload and Download transactions according to File Definitions:

```
ftp> dir
drwx------    user11  user1              0 Oct 13 09:56 FtpFiles
d-wx------    user11  user1              0 Oct 13 09:56 F41310000001
dr-x------    user11  user1              0 Oct 13 09:56 F41310000002
```

"FTPFiles" directory is a Virtual Alias parameter value which corresponds to the "c:\test2" Server directory.

Note: Files named F41380000001 and F41380000002 are examples of an error condition. They are shown here as an example of what the user may see when no Virtual Alias parameter is configured in the transfer defintion. They are the actual File IDs which user "user1" will see if no Virtual Alias parameter was configured for Upload (F41380000001) or Download (F41380000002) file definitions. We will use the correct configuration: "FtpFiles" for our example of the FTP transaction flow.

Step 3.

User "user1" performs a listing of the /FtpFiles directory in order to see the files available for transfer:

```
ftp> cd FtpFiles
ftp> dir
150 Opening data connection for file list.
-rwx------    user11  user1          79005 Apr 15 14:25 file3.txt
```

```
-rwx------    user11  user1         702188 Apr 15 14:42 file4.txt
```

Step 4.

User “user1” performs an Upload (put) of the file file1.txt from his current c:\test1 directory on the client side to the /FtpFiles directory on the Server side and then checks that the file was uploaded by listing the /FtpFile directory again:

```
ftp> put file1.txt
200 PORT command successful.
150 Opening data connection for FtpFiles
226 Transfer successful. AuditID=A41310000001
ftp: 40705 bytes sent in 0.00Seconds 40705000.00Kbytes/sec.
ftp> dir
-rwx------    user11  user1          40705 Apr 13 09:57 file1.txt
-rwx------    user11  user1          79005 Apr 15 14:25 file3.txt
-rwx------    user11  user1         702188 Apr 15 14:42 file4.txt
```

Step 5.

User “user1” performs Download (get) of the file3.txt down to the client side:

```
ftp> get file3.txt
150 Opening data connection for file file3.txt (79005)
226 Transfer successful. AuditID=A41310000002
ftp: 79005 bytes received in 0.88Seconds 90.29Kbytes/sec.
```

▲Back to Top

10 Setting up MFT FTPS Transfers

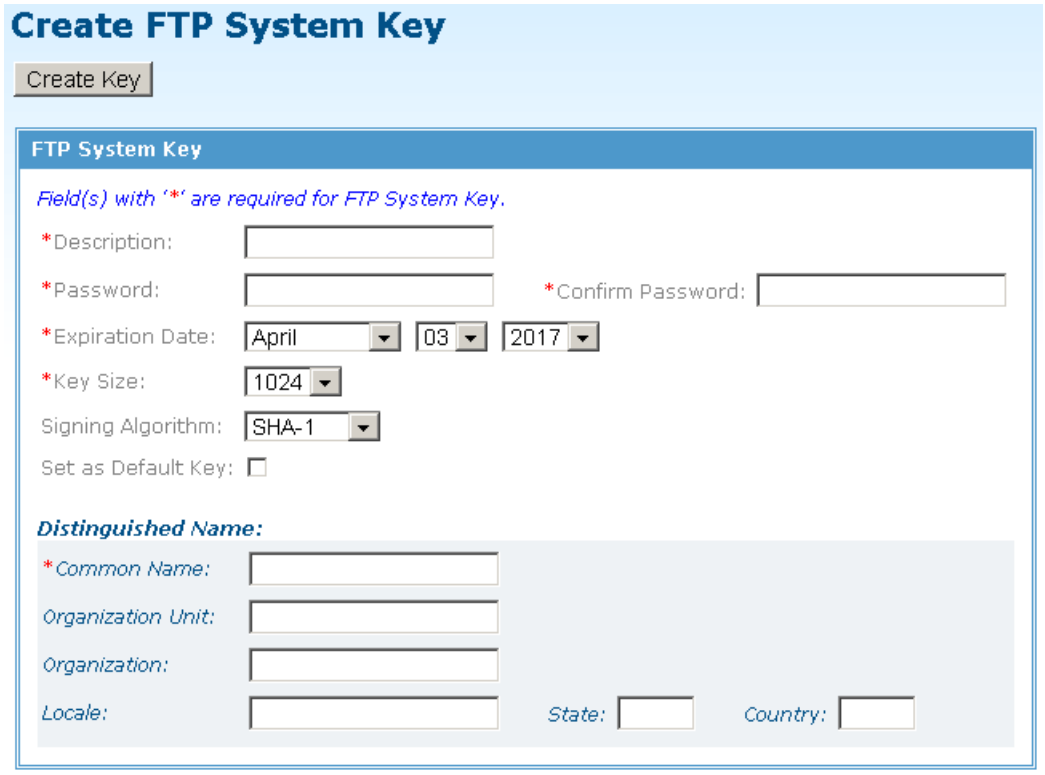
MFT Internet Server provides an internal FTP server that can be configured and used to perform FTPS transfers.

Step 1: Create an FTP System Key

All FTPS servers have a Key/Certificate pair. MFT can create the key pair for you or you may import existing keys. For our example, we will generate a new key pair for our MFT FTP Server to use as the default key pair.

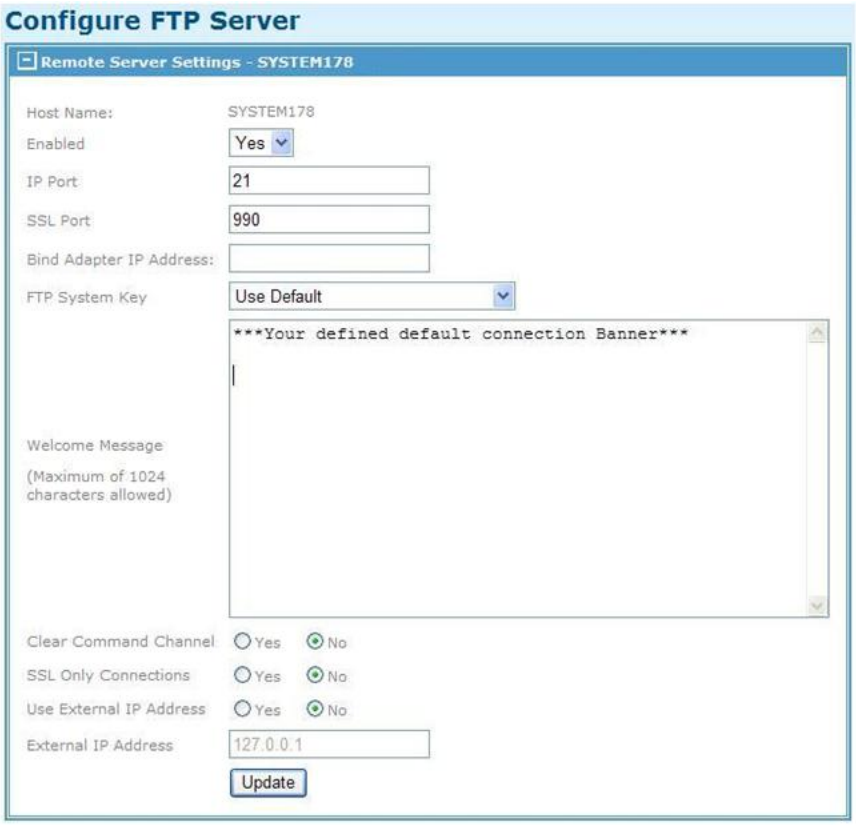
Navigate to **Administration > Keys > FTP System Keys > Create FTP Key**. Fill in the following fields to create your key:

1) **Description:** Give the key a descriptive name using this field.
2) **Password:** Give this key a password and confirm it.
3) You can accept the default **Expiration Date** and **Key Size** or edit them if you wish.
4) Check on the **Set as Default** box.
5) Add a **Common Name** under the *Distinguished Name* section.
6) Fill in the rest of the *Distinguished Name* section if desired.
7) Click on the Create Key button when you are done.



Step 2: Configure the FTP Server

Now navigate to **Administration > Transfer Servers > FTP Server > Configure FTP Server**. Expand the FTP Server Settings windows for your MFT FTP server.



Configure the following:

1) By default the server is not enabled. Change the Enabled field to read Yes.
2) By default the IP Port is set to 21, change this port if desired.
3) By default the SSL Port is disabled, change the port to 990 or desired port.
4) By default the FTP System key will be the FTP System Key you created in the first step. You may enter more keys to the MFT System and you would choose the key pair you want to use by clicking on the appropriate one from the drop down menu. For our example we are using the default key.
5) (Optional) Add a Welcome Message that users can see when they connect to the server.
6) By default the Clear Command Channel is set to No. Set to Yes if required by the network administrators.
7) By default, the FTP server will accept both FTP and FTPS connections. Set SSL Only Connections to Yes if only FTPS connections should be accepted.
8) By default, the Use External IP Address is set to No. Set to Yes if required by the network administrators.
9) Click the Update button when you are done.

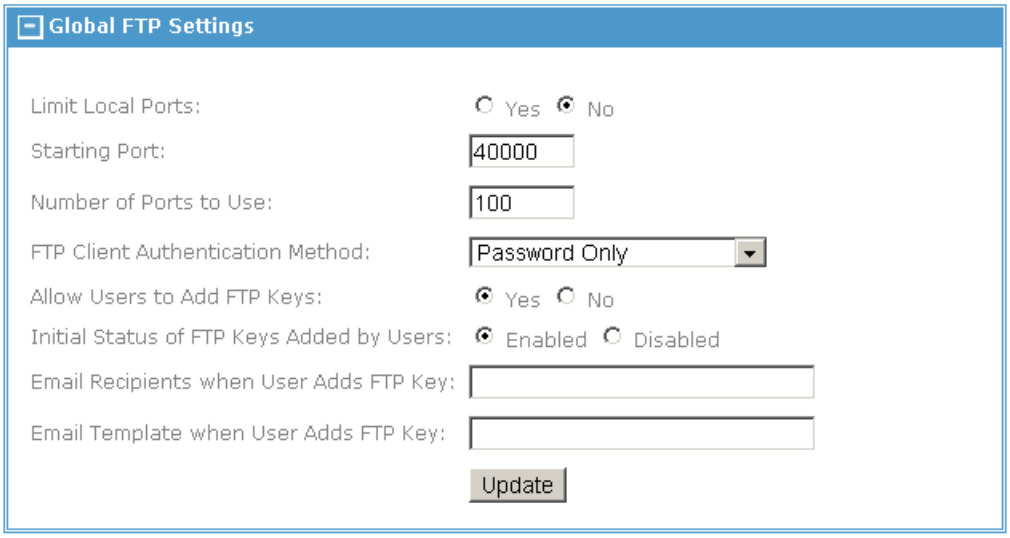
Note: Any changes made to the FTP Server Configurations page requires a restart of the service.

Step 3: Start the MFT FTP Server

Now that we have created our FTP System Key and configured our FTP server's settings we can start the server. Navigate to **Administration > Transfer Servers > FTP Server > FTP Server Status**. Click the **Start Server** button.

Step 4: Configure Global FTP Server Settings

By default the FTPS server is configured to use any available high port. Network administrators may require the FTPS server be restricted to a range of ports. Additionally, the MFT FTP Server is configured to perform *Password Only* authentication. Some environments may want to change this to *Certificate Only* authentication or use both. Navigate to **Administration > System Configuration** and expand the Global FTP Settings windows to make any changes required for your environment.



Field	Description
Limit Local Ports	If you want to restrict the FTPS server to a range of high ports, set to Yes.
Starting Port	Set the starting port number range. E.g. 40000
Number of Ports to Use	Set the port range. E.g. Number Ports = 100, sets the range 40000-40099.
FTP Client Authentication Method	Set the authentication method to be used for the MFT FTP server. Values: Password Only, Certificate Only, Certificate and Password.
Allow Users to Add FTP Keys	If you want to allow a user to add their own FTP public keys to the MFT database set this to Yes. (Users can add their FTP public keys through the Thin Client.)
Initial Status of FTP Keys Added by Users	When a user adds their own FTP public key do you want that key to be enabled or disabled
Email Recipients when User Adds FTP Key	Enter the email address(es) to be used for an email to be sent to when a user has added a new FTP Public Key to the MFT database. Separate multiple email addresses with a comma.

Email Template when User Adds FTP Key	The email template that will be used when sending out notification to the email recipient in the field above. The default email template can be found in the <WEB_Server>\cfcc\email-templates\email-ftp-key-notification-template.xml

▲Back to Top

11 Using a Local Translation Table

By default MFT Internet Server comes with two internal tables to convert ASCII to EBCDIC and vice versa. These two translation tables are used for transfers between a mainframe and Windows or UNIX platforms. There are times when the default translation table is not exactly what is needed. An administrator can define a new translation table to be used by the Local MFT Internet Server install. A customized translation table can be used for these instances.

The example below will alter the text JSY contained in a file to read CAT on the remote z/OS system.

Step 1 Create a Custom Translation Table

From the directory <MFTIS_Install>/server/webapps/<context>/translate make a copy of the Comtblg.cp037 and paste into an empty directory on the MFT Internet Server web server rename it to LTABLE.dat. This file contains the table below which converts data between the ASCII and EBCDIC and EBCDIC to ASCII character sets:

```
000102033728D2E2F1605 0A0B0C0D0E0F
101112133C3D322618193F27221D351F
405A7F7B5B6C507D4D5D5C4E6B604B61
F0F1F2F3F4F5F6F7F8F97A5E4C7E6E6F
7CC1C2C3C4C5C6C7C8C9D1D2D3D4D5D6
D7D8D9E2E3E4E5E6E7E8E9BAE0BBB06D
798182838485868788899192939495 96
979899A2A3A4A5A6A7A8A9C04FD0A107
9F000000000000000000000000000000
000000000000000000000000000000000
41AA4AB100B26AB5BDB49A8A5FCAAFBC
908FEAFABEA0B6B39DDA9B8BB7B8B9AB
6465626663679E68747172737875767 7
AC69EDEEEBEFECBF80FDFEFBFCADAE59
4445424643479C485451525358555657
8C49CDCECBCFCCE170DDDEDBDC8D8EDF
002E2E2E2E2E2E2E2E2E0A2E2E0D2E2E
2E2E2E2E2E0A2E2E2E2E2E2E2E2E2E2E
2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E
2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E
20A0E2E4E0E1E3E5E7F1A22E3C282B7C
26E9EAEBE8EDEEEFECDF21242A293BAC
2D2FC2C4C0C1C3C5C7D1A62C255F3E3F
F8C9CACBC8CDCECFCC603A23402273D22
D8616263646566676869ABBBF0FDFEB1
B06A6B6C6D6E6F707172AABAE6B8C680
B57E737475767778797AA1BFD0DDDEAE
5EA3A5B7A9A7B6BCBDBE5B5DAFA8B4D7
7B41424344454647484 9ADF4F6F2F3F5
7D4A4B4C4D4E4F505152B9FBFCF9FAFF
5CF7535455565758595AB2D4D6D2D3D5
303132333435363738 39B3DBDCD9DA2E
```

ASCII-EBCDIC portion of the translation table

EBCDIC-ASCII portion of the translation table

To make better sense of the table above we have placed it in an Excel Spreadsheet below for demonstration purposes only:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	02	03	37	2D	2E	2F	16	05	0A	0B	0C	0D	0E	0F
1	10	11	12	13	3C	3D	32	26	18	19	3F	27	22	1D	35	1F
2	40	5A	7F	7B	5B	6C	50	7D	4D	5D	5C	4E	6B	60	4B	61
3	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	7A	5E	4C	7E	6E	6F
4	7C	C1	C2	C3	C4	C5	C6	C7	C8	C9	D1	D2	D3	D4	D5	D6
5	D7	D8	D9	E2	E3	E4	E5	E6	E7	E8	E9	AD	E0	BD	5F	6D
6	79	81	82	83	84	85	86	87	88	89	91	92	93	94	95	96
7	97	98	99	A2	A3	A4	A5	A6	A7	A8	A9	C0	6A	D0	A1	07
8	9F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
A	41	AA	4A	B1	00	B2	6A	B5	BD	B4	9A	8A	5F	CA	AF	BC
B	90	8F	EA	FA	BE	A0	B6	B3	9D	DA	9B	8B	B7	B8	B9	AB
C	64	65	62	66	63	67	9E	68	74	71	72	73	78	75	76	77
D	AC	69	ED	EE	EB	EF	EC	BF	80	FD	FE	FB	FC	AD	AE	59
E	44	45	42	46	43	47	9C	48	54	51	52	53	58	55	56	57
F	8C	49	CD	CE	CB	CF	CC	E1	70	DD	DE	DB	DC	8D	8E	DF

Since we are going from an ASCII system (Windows) to an EBCDIC system (z/OS) you will be looking up the EBCDIC character for each ASCII character and replacing it with the EBCDIC character we want.

The ASCII value for J is 4A so you will go to the chart above and locate 4 going down and slide your finger to the right until you are in the A column. You will see the EBCDIC value D1 for J. We want this to translate to a C so you will replace the D1 with C3 which is the EBCDIC value for C. Do the same to have S translate to A and Y to T. Then save this file.

Step 2 Create a text file.

Create a text file containing capital JSY on your windows platform and save it to be transferred later.

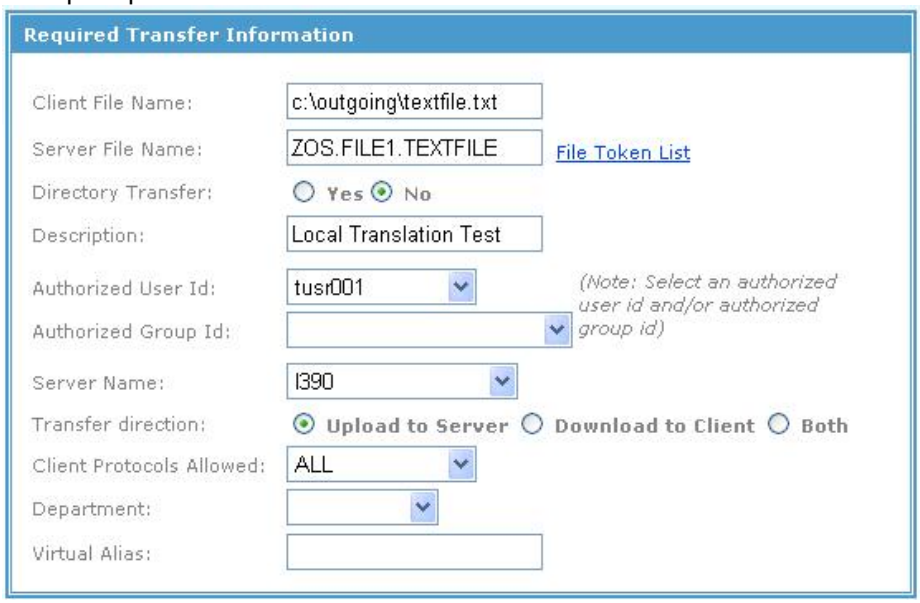
Step 3 Create an Upload File Definition

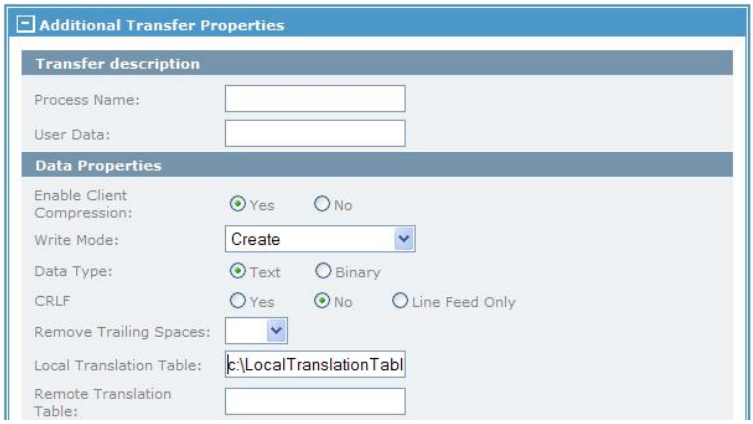
Navigate to **Transfers > Add Transfer** and fill in the *Required Transfer Information* section with the information below:

1) **Client File Name**: Type in the path of a file you created in Step 2.
2) **Server File Name**: Set the file name for the file that will be created on z/OS.
3) **Directory Transfer**: Select No.
4) **Description**: Add a short description.
5) **Authorized User Id**: Choose the user id from the drop down lists that will be used to make this file transfer.
6) **Server Name**: This is set to T390 representing our z/OS system.
7) **Transfer Direction**: Select Upload to Server.
8) **Client Protocols Allowed**: Set to ALL. (Translation tables will only be used with HTTP protocol.)
9) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.

10) Expand the section named *Additional Transfer Properties*
11) Change **Data Type** to Text.
12) Type in the path to your translation table you created in Step 1.
13) When you are done click on the Add button.

Example Upload File Definition





Now log in to the Thin Client with your MFT user id, in our case we used tusr001, and click on the Upload button. Your file written to the mainframe should contain the letters CAT and not JSY.

▲Back to Top

12 File Token Examples

MFT supports the use of file tokens in the MFT Internet Server transfer definition field called Server File Name. When a token is used it is translated to generate a new file name when it is written.
Below are examples of our most popular file tokens in use based on the following client file name:

C:\dir1\dir2\dir3\clientfile.txt

Server File Name	Resolved Server File Name
C:\dir4\#(ClientFileName)	C:\dir4\clientfile.txt
C:\serverfile.#(Date)	C:\serverfile.20081231
C:\serverfile.#(Date1)	C:\serverfile.081231
C:\serverfile.#(Date2)	C:\serverfile.123108
C:\serverfile.#(Date3)	C:\serverfile.311208
C:\#(D01)\serverfile.txt	C:\dir1\serverfile.txt
C:\#(D02)\serverfile.txt	C:\dir2\serverfile.txt
C:\#(DIR)\serverfile.txt	C:\dir1\dir2\dir3\serverfile.txt
#(DRIVE):\dir4\serverfile.txt	C:\dir4\serverfile.txt
#(FILE)	C:\dir1\dir2\dir3\clientfile.ext
C:\#(HDIR)\serverfile.txt	C:\dir1\serverfile.txt
C:\dir4\#(HLQ).doc	C:\dir4\clientfile.doc
C:\serverfile.#(JDate)	C:\serverfile.2008182
C:\dir4\serverfile.#(LLQ)	C:\dir4\serverfile.txt
C:\#(LocalUserId)\serverfile.txt	C:\jdoe\serverfile.txt
W:\#(NODRIVE)	W:\dir1\dir2\dir3\clientfile.txt
C:\#(NOHDIR)\serverfile.txt	C:\dir2\dir3\serverfile.txt
C:\#(NOSDIR)\serverfile.txt	C:\dir1\dir2\serverfile.txt
C:\#(Q01)\serverfile.txt	C:\dir3\serverfile.txt
C:\#(Q02)\serverfile.txt	C:\dir2\serverfile.txt
C:\#(RDIR)\#(ClientFileName).#(Time)	C:\dir5\success\clientfile.txt.245959999
C:\#(RFILE)	C:\dir5\success\clientfile.txt
C:\#(SDIR)\serverfile.txt	C:\dir3\serverfile.txt
C:\serverfile.#(Time)	C:\serverfile.245959999
C:\serverfile.#(Time1)	C:\serverfile.245959
C:\serverfile.#(Time2)	C:\serverfile.2459599
C:\sales.#(TransactionNumber).txt	C:\sales.IA30800003.txt

▲Back to Top

13 Using Post Processing to Delete/Rename a file on an FTP/SSH Server

In the Add Transfer Definition section of this guide we discuss setting up a file transfer definition to the system. In this example we take that further and show you how to add a Post Processing Action (PPA) to either rename or delete a file when performing a proxy to an FTP/SSH server.

For this example, let's say you want to send a file to an FTP server and upon the transfer completing you want to rename that file. We can do this by defining the following command in the Post Processing Action section of the file transfer definition:

Note: You can find a list of the all the available local PPA tokens that MFT Internet Server supports by clicking on the PPA Token List *link on the Add Transfer or Update Transfer pages after expanding the Post Processing Actions window.*

Along with the Rename command you can also perform a Delete using the following format:

Delete %LFILE

The PPA Data "Delete" and "Rename" commands can be used in the following formats:

Delete file
Rename file1 file2
FUSUTIL D file
FUSUTIL Delete file
FUSUTIL R file1 file2
FUSUTIL Rename file1 file2

▲Back to Top

14 Sending Data to a JMS Queue

The following example demonstrates how to send data to a JMS Queue through Platform Server Command Line Interface. It requires both MFT Command Center and MFT Internet Server to be installed and sharing the same database and MFT Platform Server for Windows installed. It assumes the JMS Service has been configured and started in MFT Command Center and a JMS queue named, MFT.Queue1, has been created on JMS.

Step 1: Add Server Definition of Server Type JMS

Navigate to **Servers > Add Servers**

Fill in the required fields as shown below:

1) **Server Name**: This can be any name
2) **IP address**: Type the address 127.0.0.1. Note: This is a required field but is ignored for JMS since the JMS connectivity information is defined in the Configure JMS Service web page.
3) **Server Type**: Set to JMS

Step 2: Add Server Definition of Server Type Internet Server

Navigate to **Servers > Add Servers**

Fill in the required fields as shown below:

1) **Server Name**: This can be any name
2) **IP address**: Type the address of the Internet Server.
3) **IP Port**: Type the port the Internet Server is listening on. This is typically secure port 443
4) **Server Type**: Set to Internet Server

   Scroll Down and expand the Internet Server Options box and set the context name being used by the Internet Server. If you are unsure this information can be found under the System Configurations menu in the Remote Settings for the Internet Server installed.

Step 3: Add Transfer Definition

Navigate to **Transfers > Add Transfers**

Fill in the required fields in the sections as shown below:

Required Transfer Information

1) **Client File Name**: This can be anything.
2) **Server File Name**: Set this field to MFT.Queue1. Note: If you want to make this dynamic you can use the #(FileName) token.
3) **Directory Transfer**: Select No.
4) **Description**: Add a short description.
5) **Authorized User Id**: Choose the user id from the drop down list that will be used to make this file transfer. Note: The user must have TransferRight assigned to his user account.
6) **Server Name**: Select the JMS server defined in step 1.
7) **Transfer Direction**: Select Upload to Server.

8) **Client Protocols Allowed**: Set to ALL
9) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.
10) **Virtual Alias**: Add the alias that the client will use for transfers. In this example use JMSUP.

Additional Transfer Properties (expand this section)

11) **Data Type**: Set this value to Text. This tells the system to write Text data to JMS (Queues used by the BW Interface require Text data). Binary tells the system to write Byte data to JMS
12) **CRLF**: Tells the system how to handle record delimiter

No	All data will be written to JMS as a single message.
Yes	Data will be split into individual JMS Messages when CRLF is found
LF	Data will be split into individual JMS Messages when LF is found

JMS Properties (expand this section)

13) **Input Selector**: Ignored for upload requests.
14) **Output JMSType Property**: Set to JMSUpload. Defines the JMS Type Output Property that is written when the file is sent to the JMS queue.
15) **Max Message Size**: Specify a maximum message size. (1K-999K, 1M-10M: default=1M). When a message exceeds this size it will be broken up into multiple messages.
16) When you are done click on the Add button.

Step 4: Send data from client to the JMS Queue

Open the Command Prompt and navigate to the Platform Server's Command Line Interface. Below is a command using the settings above to send the file to JMS:

ftmscmd /send /file /destination:10.97.142.154 /port=46464 /remoteuserid=jmsuser /remotepassword=pwd c:\outgoing\testfile.txt JMSUP/MFT.Queue1

Note: Due to the transfer definition parameter, **Client Protocols Allowed**, being set to ALL this upload can also be performed by an FTP Client, an SSH Client, the Thin Client, and the Desktop Client if configured.

▲Back to Top

15 Receiving Data from a JMS Queue

The following example demonstrates how to receive data from a JMS Queue. This example assumes the JMS Service in Command Center has been configured and is started (refer to the Command Center User Guide for more information). It also assumes a JMS queue named “MFT.Queue1 has been created in JMS.

Note: Sending data to a JMS Queue requires both MFT Command Center and Internet Server.

Step 1: Add Server Type JMS

Navigate to **Servers > Add Servers**

Fill in the required fields as shown below:

1) **Server Name**: This can be any name
2) **IP address**: This is a required field for Add Server. The field is ignored for JMS since the JMS connectivity information is defined by the Command Center.
3) **Server Type**: Must be JMS

Step 2: Add Transfer definition

Navigate to **Transfers > Add Transfers**

Fill in the required fields in the sections as shown below:

Required Transfer Information

1) **Client File Name**: This can be anything.
2) **Server File Name**: Set this field to the name of the queue you want to write. If you want to make this dynamic you can use the #(FileName) token. In this example enter MFT.Queue1.
3) **Directory Transfer**: Select No. Downloads require transfers to be file transfer not directory.
4) **Description**: Add a short description.
5) **Authorized User Id**: Choose the user id from the drop down lists that will be used to make this file transfer. The user must have transfer right.
6) **Server Name**: Select the JMS server defined in step 1.
7) **Transfer Direction**: Select Download to Client.
8) **Client Protocols Allowed**: Set to ALL
9) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.
10) **Virtual Alias**: Add the alias that the client will use for transfers. In this example use JMSDOWN.

Additional Transfer Properties (expand this section)

11) **Data Type**: This field is ignored when reading from a JMS queue.
12) **CRLF**: Tells the system how to handle record delimiter

No	All messages will be read from JMS and written as a single record
Yes	CRLF delimiters will be added at the end of each JMS message read
LF	LF delimiters will be added at the end of each JMS message read

JMS Properties (expand this section)

13) **Input Selector**: Filters data when reading a JMS Queue. Default is to read all data in a queue.
14) **Output JMSType Property**: This parameter is ignored on download requests and can be left blank.
15) **Output Property**: This parameter is ignored on download requests and can be left blank.
16) Max Message Size: This field is ignored on a download.
17) When you are done click on the Add button.

Step 3: Receive data from the JMS Queue to a client

Go to the client from which the data will be sent. The following example assumes a JMS Queue "MFT.Queue1" has been defined in JMS. FTP Command Line is the client in this example; however any client could be used.

FTP to the MFT Internet Server and authenticate with the JMSuser credentials
get /JMSDOWN/MFT.Queue1 c:\test.txt

▲Back to Top

16 Installing the Internet Server's Thin Client

MFT provides several mediums to conduct file transfers with. One of these is the Internet Server's web browser client called the Thin Client. The client allows you to transfer files through your browser. The client requires Sun's Java plug-in to be installed.

6.1 Sun Java Plug-in (required by Thin Client)

The Sun Java plug-in, version 1.6.0_xx, must be downloaded and installed for a Transfer User to execute Internet Server Transfers. The Internet Server Transfer client is designed to download the Sun Java plug-in the first time the end-user executes the screen.
Optionally:

The Java plug-in can be downloaded from the Sun web page (http://java.sun.com) and select J2SE v 1.6.0_ xx. Make sure the client has authority to download and install the Java plug-in.

Access the Java plug-in using the web page provided with MFT Command Center. (https://[DNS_HostName]:[httpsPort]/cfcc/control?view=download/setup.jsp) Make sure the client has authority to download and install the Java plug-in

6.2 Disable Caching

After downloading the Java plug-in, TIBCO suggests that you disable caching.
In Windows:

Go to the Control Panel and double click on the Java plug-in icon. Select the General tab and click the Settings button in the Temporary Internet Files Frame. On the Temporary Files Settings window, uncheck the Keep temporary files on my computer checkbox and click OK. Click OK again to close the Java Control Panel.

Once you have the Java plug-in installed and disabled caching the following URL can be used to login and use the Thin Client (to conduct transfers with this client a transfer definition needs to be defined, see Section 5 for more details):

https://[DNS_HostName]:[httpsPort]/cfcc/control?view=view/filetransfer/thin/start.jsp

▲Back to Top

17 Using the Thin Client

A user logs on to the Thin Client and a screen similar to the one below will be displayed. At the top of the screen are icons labeled Transfers, History, Change Password, Keys and Help. The Thin Client will display a list of the transfers for the logged on user by default.

Icons:

Transfers: refreshes the list of File Transfers that are ready for the user to execute.

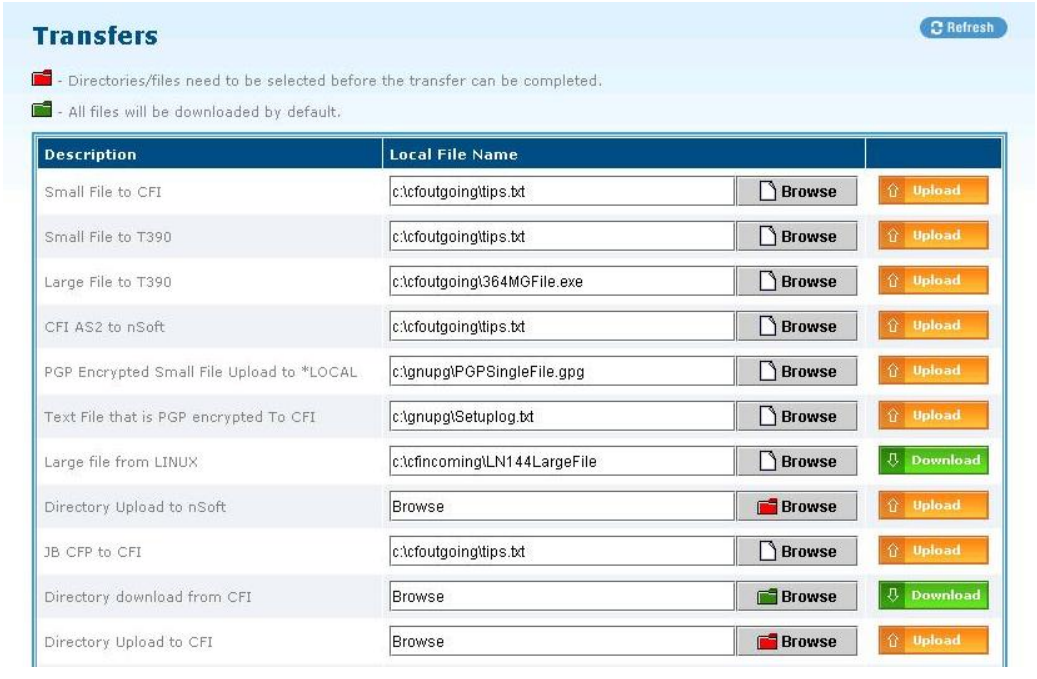
History: displays the most recent file transfers that have been executed by this user.

Change Password: allows the user to change the MFT Command Center password.

Keys: displays the default PGP, SSH, and FTP system keys for MFT and allows users to add their own keys.

Help: provides some general help information about the file transfer screens.

The “Refresh” button refreshes the data in the screen that you are in. If you are in the Transfers screen, it will refresh the list of transfers. If you are in the History screen, it refreshes the list of completed transfers.



Field	Description
Description	Additional information about the transfer, defined by the MFT Command Center Administrator.

Field	Description
Local File Name	**Upload:** **Local File Name** displayed should be the same as the file name and location on your computer. If this is not correct, click **Browse** to search for the correct file to upload. **Download:** **Local File Name** is the name that the file will have when it is downloaded and saved to your computer.
	The white file icon indicates you are to transfer a single file. To upload a file, enter the file's path and name, or click **Browse** to select the file from the Network. Press **Upload** under to begin transfer. To Download a file, click **Browse** and choose the location to save the file, if different from the path and file name displayed. Press **Download** to begin transfer.
	The red Folder icon indicates that you are able to transfer all files in a Directory. Click **Browse** to search for Directories. You may select a single file, or click on "Select All" to transfer all files in a directory. Press **Upload** to start file transfer. To **Download** files from the source directory, click **Browse**. The left side displays the directories available for download. The right side of the panel shows the files available on the MFT Command Center Server. Server file names cannot be changed. You may choose particular files or click **Select All** button to select all the files listed. Press **Download** under to start file transfer.
	A green Browse folder icon indicates a directory Download that may have been configured with a default download location where all available files will be transferred. The default location is specified in the Local File Name column located left of the Browse button. If you want to change the predefined location simply click on the Browse button to select a new location or click inside the Local File Name box and type in a location.
Click to Transfer	Click to start file transfer. The button will show either **Upload** or **Download**. **Upload** to send the file **Download** to receive a file.
Execute all Transfers	Click this button to process (upload/download) all Transfers displayed on the screen

7.1 History

Click on History to view a record of the most recent transfers processed under your account.

Field	Description
Audit ID	A unique identifier for this audit record generated by the MFT Command Center system.
Status	Transfer success or failure.
Local File Name	The name of the file that was transferred.
Description	Additional information about the transfer, defined by the MFT Command Center Administrator.
Direction of Transfer	Upload or Download.
Transfer Date	Date of transfer.
Bytes Transferred	The number of bytes transferred.

7.2 Change Password

Click on Change Password to change your password, as warranted.
End-users can change only their own passwords.

7.3 Keys

Click on Keys to retrieve the system keys used for PGP, SSH and FTP. Users can also upload their own keys that can be used for PGP encryption, and SSH and FTP authentication.

7.4 Help

Help provides some general help information about the file transfer screens.

▲Back to Top

18 Installing the Desktop Client

MFT Internet Server comes with the new MFT Desktop Client ClickOnce application. By utilizing the Microsoft ClickOnce technology within our MFT Desktop Client it enables users to install, update and run the MFT Desktop Client with minimal user interaction and no Administrator requirements. The Desktop Client ClickOnce application requires some customization steps to be performed before making it available to end users to download and install. Windows SDK is required for the customization process. Please refer to the MFT Internet Server Installation Guide, for detailed instructions to customize this application for you environment.

Once you have installed the customized Desktop Client it is ready for end users to connect to the system and download it to install on their systems. There are two types of installations offered. The first is a full install offered where the end user would install the Desktop Client program on to their desktop. The other is a cached install where the Desktop Client would be initiated each time from the end user's browser. The end user must choose the one that will work best for their environment.

8.1 Desktop Client Program Install

To connect and have the MFT Desktop Client program installed on an end user's desktop we have a full URL as well as a shortcut that can be used. Below is the format of the full URL:

https://[DNS_HostName]:[httpsPort]/[context]/client/install.html

The shortcut URL that an end user can use to connect and install the MFT Desktop Client is as follows:

https://[DNS_HostName]:[httpsPort]/desktop-install

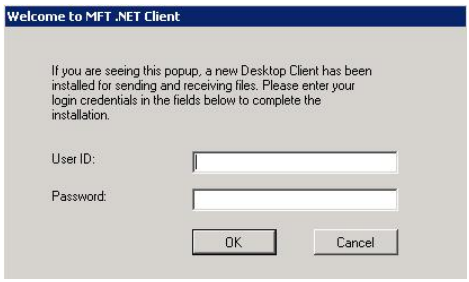
Note: When using the shortcut URL and an Internet Explorer 7, 8, or 9 browsers the end user must enable "Automatic prompting for file downloads" by opening the Internet Options window and clicking on the Security tab. Click to highlight the **Internet** zone to edit. Then on the same panel click **Custom level** button. The Security Settings – Internet Zone window will open. Scroll down until you see "Automatic prompting for file downloads" and set it to **Enable**. Click the **OK** button. Then click the **Apply or OK** button again and refresh your screen.

The following MFT Desktop Client install web page will be displayed:

Click on the Install button to have the MFT Desktop Client download and install on the end user's desktop.

The TIBCO MFT Desktop Client License Agreement window will be displayed next. Click on the **Accept** button.

When the download and install has completed the end user will be presented with the following Welcome window to enter their userid and password to login with:



If the end user does not want to login at this time they can click on the Cancel button and try again later by clicking on their Start menu and navigating to Start > Programs > MFT Desktop Client.

8.2 Browser Based Desktop Client Install

Just like the MFT Desktop Client program install the cached version of the MFT Desktop Client can be installed by using either a full URL or a shortcut. Below is the format of the full URL:

https://[DNS_HostName]:[httpsPort]/[context]/client/cache.html

The shortcut URL that an end user can use to connect and install the MFT Desktop Client is as follows:

https://[DNS_HostName]:[httpsPort]/desktop

Note: When using the shortcut URL and an Internet Explorer 7, 8, or 9 browsers the end user must enable “Automatic prompting for file downloads” by opening the Internet Options window and clicking on the Security tab. Click to highlight the **Internet** zone to edit. Then on the same panel click **Custom level** button. The Security Settings – Internet Zone window will open. Scroll down until you see “Automatic prompting for file downloads” and set it to **Enable**. Click the **OK** button. Then click the **Apply or OK** button again and refresh your screen.

▲Back to Top

19 Setting up AS2 Connections with Trading Partners

Step 1: MFT AS2 Server Configurations

Navigate to **Management > System Servers > AS2 Server > Configure AS2 Server**. Expand the AS2 Server Settings windows for your MFT AS2 server. Configure the following:

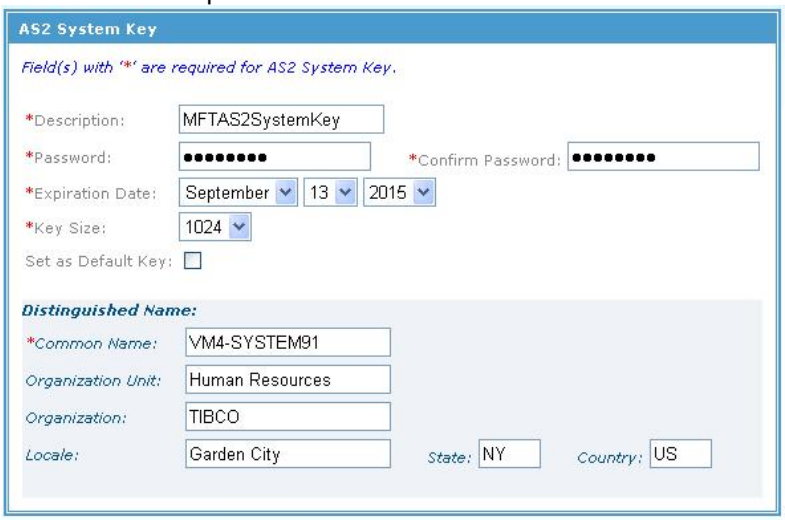
1) By default the server is not enabled. Change the **Enabled** field to read **Yes**.
2) Both the **Receive URL** and **Async Response URL** need to be edited.
    a. In both fields edit "yourserver" to read your server name.
    b. Change "port" to your web server's non-ssl port number. Most commonly used port numbers for this are 8080 for Tomcat, and 9080 for WebSphere. Your environment may be configured differently. Check with your web administrator.
3) If your AS2 server protocol requires a Proxy server you will need to configure the Proxy Information section. (This is rarely used.)
4) Define the **Local AS2 ID**. This will become your default AS2 ID. Note: You can define another Local AS2 ID in the Server definition if needed. The Server definition will override what is configured in this field.
5) Click on the Update button when you are finished to save the changes.

Step 2: Create an AS2 System Key

Navigate to **Management > Keys > AS2 System Keys > Create AS2 Key**. Fill in the following fields to create your key:

1) **Description**: Give it a descriptive name using this field.
2) **Password**: give this key a password and confirm it.
3) You can accept the default **Expiration Date** and **Key Size** or edit them if you wish.
4) Check on the **Set as Default** box.
5) Add a **Common Name** under the *Key Distinguished Name* section.
6) Fill in the rest of the *Key Distinguished Name* section if desired.
7) Click on the Create Key button when you are done.

Below is an example:



Now Navigate to **Management > Keys > AS2 System Keys > Manage AS2 Keys** and click on the one you created above to see the AS2 Public Certificate you will copy to send to your Trading Partner in Step 4.

Step 3: Creating a MFT User ID for AS2 Incoming requests

Each Trading Partner can have an AS2 user id that will be associated with their AS2 incoming requests.
Navigate to **Users > Add User** to create the new user. You must set this user's Client Protocols in the Optional User Properties section to AS2, (Setting the Client Protocols to All does NOT include AS2). If you need help creating a user id go to section *Add User* from the MFT Command Center User Guide. This user id will be used in Step 5 when you create an AS2 Server in this example. If you don't create the user id now you will have an opportunity later in Step 5 using the *Create User for Incoming AS2 Requests* link from the Server definition.

Step 4: Exchanging AS2 Server communications data with AS2 Trading Partners

Now you have to exchange information with your AS2 Trading Partner that you will be communicating with. Below is both the information you need to obtain from your Trading Partner and information that you will give to your Trading Partner:

Information you need from your Trading Partner:
1) Their Partner AS2 ID (AS2 Identifier)
2) Their AS2 URL.
3) Their Public Encryption Certificate and/or their Signing Certificate in a Base64 format. (In most cases you only need the Encryption Public Certificate.)

Information you will give to your Trading Partner:
1) Your Local AS2 ID that you created in Step 1.
2) Your Receive URL you configured in Step 1.
3) Your AS2 Public Certificate that was created in Step 2.

Once you have all the information above you can move on to Step 5.

Step 5: Add a Server Definition for your Trading Partner to MFT Command Center

You need to add your Trading Partner to MFT Command Center. Navigate to **Servers > Add Server** where you will see the following at the top of the web page:

Fill in only the fields listed below. All other fields should not be changed:
1) **Server Name**: A descriptive name for this AS2 Server.
2) **IP Name**: Must contain the partners URL you requested from the Trading Partner in Step 4.
3) **Server Type**: Should be set to AS2.

Then scroll down and expand the *AS2 Options* section. Most of the fields you can leave configured with the default information which we will be doing for our example. Fill in the fields listed below with the following information:

1) **Partner AS2 ID**: Place your Trading Partner's Id you received in Step 3.
2) **User ID**: This is the MFT User that will be associated with all incoming AS2 requests from the Trading Partner. This is the user id that was created in Step 3 of this example. If you did not create a user id in Step 3 you may do so now by clicking the *Create User for Incoming AS2 Requests* link. When you have finished you can click on the back button to get back to this page and F5 to refresh.
3) **Encryption Public Certificate** in the *Partner Public Certificate* section you would place the Base 64 certificate you would have received from your Trading Partner in Step 4. If they sent you a Base 64 Signing Public Certificate you can add it in its appropriate section as well.
4) Accept all other defaults and click on the Add button. You will see a successful message along with a link for the next step.
5) Click on the *Create Transfer Definition for Incoming AS2 Requests* and continue to Step 6.

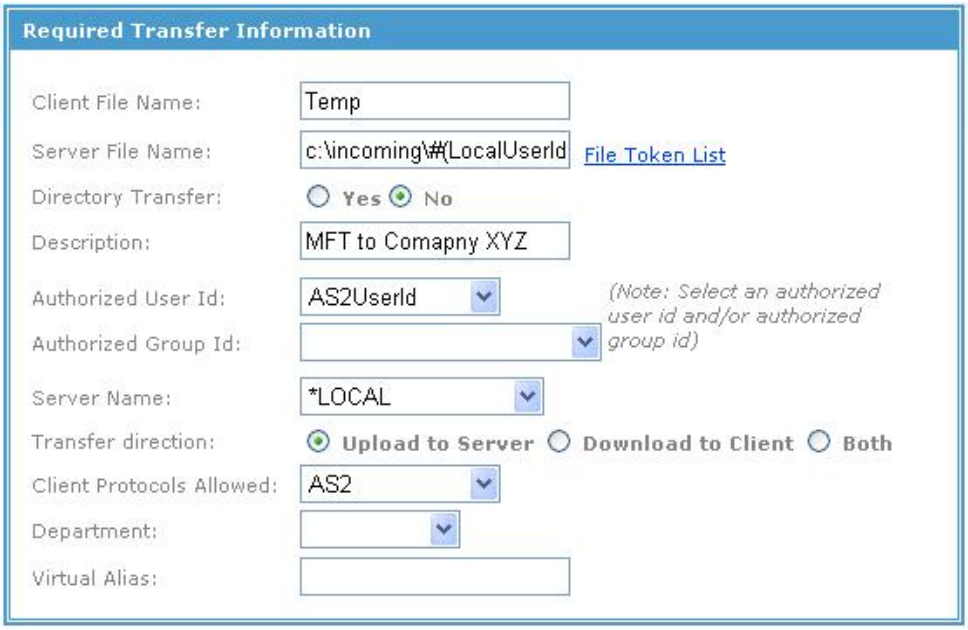
Step 6: Create AS2 transfer definitions

Step 6.a Receiving a file from your Trading Partner (Incoming Requests):

To allow the Trading Partner to send a file to MFT Internet Server you would need to setup an upload file definition. By clicking on the link in the prior step you were brought to a transfer definition template. You can also get to this web page by Navigating to Transfers > Internet Transfer > Add Transfer. You will see the *Required Transfer Information* section open. Fill in the information below in the following fields:

5) **Client File Name**: For AS2 incoming transfers we don't use this field so we will place Temp.
6) **Server File Name**: Set the path and file name for the files that will be written. We suggest you add to your Server File Name path the date and time File tokens. This will ensure that incoming files are unique.
7) **Directory Transfer**: Set to No. (This could be set to Yes, but our example is sending a single file.)
8) **Description**: Add a short description users will see when they log into the Thin Client.
9) **Authorized User Id**: Must be changed to the AS2 user Id you created in Step 3.
10) **Server Name**: Choose the Server where you want the files sent. (In our example we will be receiving files to the *LOCAL MFT server.)
11) **Transfer Direction**: Select Upload to Server.
12) **Client Protocols Allowed**: Leave as AS2.
13) Click the **Add** button to create the transfer definition.

Below is our example:



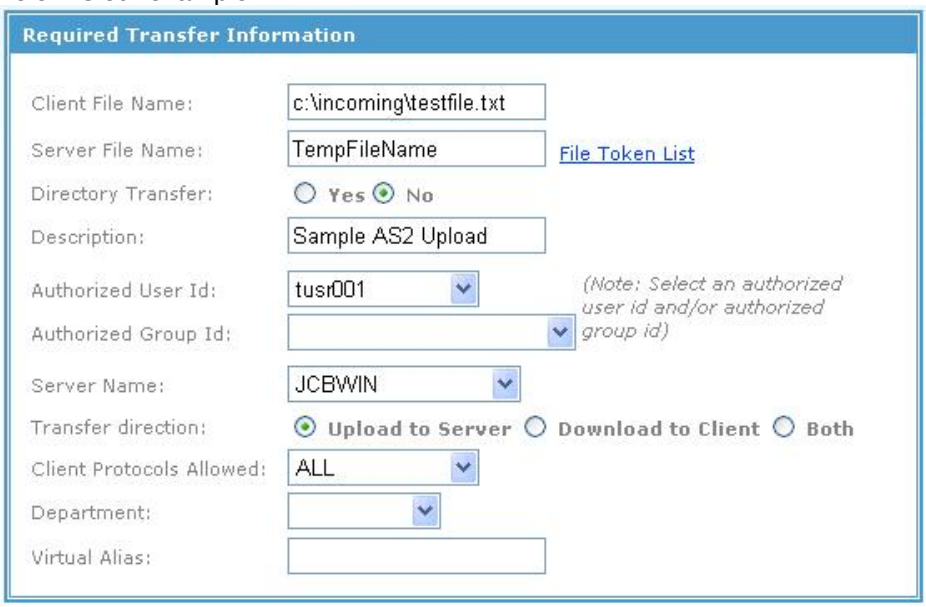
Now when you're trading partner sends a file to you it will be written to the Local MFT server into directory c:\MFTncoming\#(LocalUserId)#(Time1)#(ClientFileName).

Step 6.b Sending a file to your Trading Partner (Outgoing requests):

Now we will create an upload file definition for a user to send a file to your Trading Partner. Navigate to **Transfers > Internet Transfer > Add Transfer** and fill in the *Required Transfer Information* section with the information below:

1) **Client File Name**: Set the default client file name that will be seen by the end client.
2) **Server File Name**: Set the file name that will be passed to the AS2 file server.
3) **Directory Transfer**: Select No. (This could be set to Yes, but our example is sending a single file.)
4) **Description**: Write a description for yourself that the user will see when he/she logs into the Thin Client.
5) **Authorized User Id** or Group: Choose the user id or group from the drop down lists that will be initiating this transfer.
6) **Server Name**: Choose the AS2 server where you want to send the AS2 request.
7) **Transfer Direction**: Select Upload to Server.
8) **Client Protocols Allowed**: Leave as ALL.
9) **Department**: If you have a department for this transfer to be assigned set it here if not leave it blank.
10) **Virtual Alias**: If you will be using an SSH, FTP or MFT Platform Server Client to upload this file add an Alias.
11) When you are done click on the Add button.

Below is our example:



User tusr001 can now log on to MFT through the Thin Client and upload testfile.txt to your AS2 Trading Partner.

▲Back to Top