TIBCO MFT Internet Server Installation 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, 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

1

Pre-requisites

Please note that support is provided for TIBCO's Managed File Transfer Internet Server only when used with an indicated third party vendor's generally supported release versions. Once the operating system or other software component goes into extended support mode, or the vendor no longer supports a version, it will cease to be supported by TIBCO Technical Support. Please see the following sections for additional information on supported operating system, database system, Java, and other software components.

Minimum Operating System Version

One of the following minimum operating systems level or above that runs the appropriate Java version (see section C) and is supported by the vendor:

HP HP-UX
  11i v1 (B.11.11), 11i v2 (B.11.23), 11i v3 (B.11.31)
  64-bit on Itanium
  11i v2 (B.11.23), 11i v3 (B.11.31) 32-bit on Itanium
IBM AIX
  6.1, 7.1 64-bit on pSeries
Microsoft Windows
  7, 8, Vista, XP 32-bit on x86
  7, 8, Vista, XP 64-bit on x86-64
  8 32-bit on x86-64
Microsoft Windows Server
  2008 32-bit on x86
  2008, 2008 R2, 2012 64-bit on x86-64
  2012 32-bit on x86-64
Novell SUSE Linux Enterprise Server
  9.0, 9.3, 9.x, 10.0, 10.1, 10.2, 10.3, 10.x, 11.0, 11.x
  32-bit on x86
  9.0, 9.3, 9.x, 10.0, 10.1, 10.2, 10.3, 10.x, 11.0, 11.x
  64-bit on x86-64
Red Hat Enterprise Linux Server
  5.x, 6.x 32-bit on x86
  5.x, 6.x 64-bit on x86-64
Sun Solaris
  10 32-bit on SPARC
  10 32-bit on x86
  10 64-bit on SPARC
  10 64-bit on x86-64

Windows XP Service Pack 2, Windows 2000 Server and Professional, and Windows 2003 Server R2 reached end of support in July, 2010. Customers should migrate to supported versions of Windows Client and Windows Server because in the event that you encounter an issue/outage in your environment on an unsupported

product, Microsoft engineers may not be able to help resolve the issue until you've upgraded to a supported level.

Minimum Database

A database created on one of the following supported databases:

Note: Databases for MFT should support a UTF-8 character set and have a case insensitive collation.

- **Microsoft SQL Server 2008 R2, 2008.x, 2012, 2014** (Using either Windows or SQL Authentication) - Customers must provide the MSSQL JDBC driver. The driver can be downloaded from http://sourceforge.net/projects/jtds/files/. Supported database driver is jTDS 1.2.5. Note: There are two zip files you can download, jtds-1.2.5-src.zip and jtds-1.2.5-dist.zip. Download the distribution file, jtds-1.2.5-dist.zip, and place it in a temporary directory. Extract all the files and verify jtds-1.2.5.jar is there.
- **MySQL 5.5.x, 5.6.x** - Customers must provide the MySQL JDBC driver. The driver can be downloaded from http://ftp.plusline.de/mysql/Downloads/Connector-J/. Supported database drivers are v.5.1.14, v5.1.15 or v5.1.16.
- **IBM DB2 for Linux, Unix and Windows 9.8.x, 10.1.x, 10.2.x** - Customers must provide the DB2 JDBC driver(s). The driver can be copied from your DB2 database. Navigate to <DB2-HOME>\java directory. If you are using DB2 v9.5 and above copy db2jcc.jar and paste it in a temporary folder that you will point to later during the installation. If you are using a DB2 version earlier than 9.5, copy db2jcc.jar, db2jcc_javax.jar, and db2jcc_license_cu.jar and paste them in a temporary folder that you will point to later during the installation.
- **Oracle Database 11g 11.1.x, 11.2.x** (Oracle 10.2 standard support ended in July 2010) - Customers must provide the Oracle JDBC drivers which can be downloaded from http://www.oracle.com/technetwork/database/features/jdbc/jdbc9201-092698.html.

  Notes for Oracle database use:
  - The Oracle RAC Single Client Access Name (SCAN) for Oracle Real Application Clusters is not supported. The following url provides additional information: http://www.oracle.com/technetwork/database/clustering/overview/scan-129069.pdf

Java

The appropriate 32-bit or 64-bit Java JDK/SDK must be installed as determined by the server architecture:

- Oracle Java 1.6.x, 1.7.x, 1.8.x
- IBM Java 7. IBM Java 7 must be used for FIPS 140-2 compliance. FIPS 140-2 support is available on z/Linux, Linux, and AIX platforms using IBM Java. You can check and compare the build date of your Java installation by using the command: `/usr/java7_64/jre/bin/java -fullversion`

Java JDK must have the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files installed. Download and follow the instructions distributed with the policy files:

- Oracle JDK policy files: http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- IBM Java JDK policy files for 256bit encryption: https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

Java Heap Size

- Default Minimum 512 MB
- Default Maximum 1024 MB or 50% of installed RAM (up to 1.2GB for 32-bit server). If a maximum value is specified greater than available RAM, the MFT Internet Server may fail to start.

To edit the settings on a UNIX system open the file <MFTCC_Install>\server\bin\setenv.sh
To edit the settings on a Windows system double click the following executable: <MFTCC_Install>\server\bin\MFT_Command_Centerw.exe. When the Command Center Properties windows opens, click on the Java tab where the default settings can be changed.

JMS (Optional – Requires MFT Command Center)

MFT Command Center Administrator interface can be configured to work with one of the following JMS servers:

- TIBCO EMS Server v6.3
- Apache Active MQ v5.5.1
- IBM MQ Series v7.1

Each JMS server install contains jar files generally in the <JMS_Install>\java\lib directory needed by both MFTCC and MFTIS. These files must be copied from the JMS server and placed in the <MFTIS_Install>\server\webapps\cfcc\WEB-INF\lib directory upon installation. Below is the JMS jar files needed for the following tested JMS Servers:

- TIBCO EMS Server 6.3
  - jms-2.0.jar (If using EMS Server version 8.0)
  - slf4j-api-1.4.2.jar
  - slf4j-simple-1.4.2.jar
  - tibcrypt.jar
  - tibjms.jar
- ActiveMQ 5.5.1
  - activemq-all-5.5.1,jar
  - slf4j-log4j12-1.5.11.jar
- IBM MQ WebSphere Series 7.1
  - com.ibm.mq.commonservices.jar
  - com.ibm.mq.headers.jar
  - com.ibm.mq.jar
  - com.ibm.mq.jmqi.jar
  - com.ibm.mq.pdf.jar
  - com.ibm.mqjms.jar
  - connector.jar
  - dhbcore.jar
  - mqcontext.jar (May have to download from the IBM web site. The following URL was used at the time of testing. http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24004684&loc=en_US&cs=utf-8&lang=en)

Browsers

The MFT Internet Server Administrator interface is supported on the following browsers:

- Apple Safari 5.1.x, 6.0.x, 7.0.x
- Google Chrome 43.0.x 44.0.x 45.0.x
- Microsoft Internet Explorer 8.0.x, 9.0.x, 10.0.x, 11.0.x
- Mozilla Firefox 38.0.x 39.0.x 40.0.x

LDAP

One of the following LDAP Directories may be optionally used for authentication in addition to the default MFT Internet Server database:

- SUN One Directory Server 6.0.x and above
- IBM Tivoli Directory Server 6.2 and above
- Microsoft Active Directory Windows 2008, 2008 R2, 2012, or 2012 R2
- Novell eDirectory 8.8.x and above

Network

As with any enterprise application, changes may need to be made to firewalls and other security systems in a production environment. The following tables list default ports for services required and used within MFT Internet Server. Please note that these are the default ports, you will need to check with the appropriate systems administrator to ensure these ports are used in your enterprise.
Either http or https can be used for soap calls. By default TIBCO MFT Internet Server uses ports 80 and 443 for http and https respectively. These defaults can be changed at installation time.

Database	Default Port
MS SQL Server	1433
Oracle	1521/1522
MySQL	3306
IBM DB2	50000

Minimum Hardware

Platform	Minimum Hardware Requirements	Minimum RAM Requirements
z-Series	Any Hardware supporting z/Linux	2 GB
p-Series	Power Family Processor	2 GB
HP	PA-RISC or Itanium processor	2 GB
SUN SPARC	Solaris compatible SPARC processor at 440 MHz	2 GB
SUN x86	x86 processor at 2.5GHz	2 GB
Linux	x86 processor at 2.5GHz	2 GB
Windows	x86 processor at 2.5GHz	2 GB

Disk Space Recommendation

Internet Server
1 GB

Database Table Space Requirements

Database	Disk Space
Low volume	100 MB
High volume	1 GB +

There are many factors that should be considered when planning and allocating database disk space. The most significant include:

1. The number of audit records that will be written from Internet Server
2. How long audits be retained in the database
3. The size of the audit records

The actual size of the audit record depends on a number of factors including the length of file names, number and size of post processing actions, number and size of email notification addresses, etc. Most audit records will range from 1 to 4 KB in size with an estimated average of approximately 2 KB. A 4 KB audit record would normally be considered very large. Using 2 KB as an average, for example, 10 GB of disc space would be enough to retain approximately 5 million audit records in the database.

Sizing Guidelines

Hardware sizing guidelines are provided in the following sections based on general rules of thumb and previous experience. There are many factors that should be considered to appropriately size required hardware and we have tried to balance the need to provide simple guidance while minimizing complexity. Therefore, these

guidelines are not guarantees of actual performance. Every deployment has unique factors that must be considered.

In addition to the above minimum requirements:

- For managing up to 100 Server nodes, two or more processor cores at 2.5 GHz or faster
- For managing up to 200 Server nodes, four or more processor cores at 2.5 GHz or faster
- One additional processor core at 2.5 GHz or faster when implementing SOAP calls
- Please consult TIBCO for information outside of the above guidelines

The default MFT Internet Server maximum database connection parameter value is set during installation to 400. For high volume file transfer environments, increase the parameter above the default of 400. The database maximum connections parameter should match the MFT Internet Server maximum database connection. Please refer to your database manual for information on how to set this parameter.

2

Creating the Database

MFT Internet Server provides a utility that will create and populate the database tables needed by MFT Internet Server. However, before running the install program, you must create a MFT Internet Server database in whichever database application you have chosen to use (See supported databases in *Section 1 Pre-Requisites*).

Have your Database Administrator create a database and a username/password on the server that will host the MFT Internet Server database tables. It is recommended that the database and username be named “cfcc”, but this is not required. This username must have the ability to read, write, and create tables in the MFT Internet Server database. The exact steps to accomplish this step vary significantly depending on the database application you are using; consult the documentation provided by your database vendor on how to perform this step.

Note:

- Database password must not contain an equal(=) sign.
- MSSQL Server Properties can be configured under the Security tab to do authentication via "SQL Server or Windows". The default is "Windows" only.
- If you are using an IBM DB2 database, you must do the following. Note that the Database, Buffer Pool and Table Space names defined below are suggested values. You can substitute names that follow your naming standards if necessary. The changes should be made through the IBM DB2 Control Center or an equivalent tool.
    - Create a DB2 database. The only required value is the database name. For example, you can assign a database name such as MFTIS DB.
    - Create a DB2 Buffer Pool with a page size of 32K. Assign a name such as MFTISBP to the buffer pool. This buffer pool will be needed in later steps.
    - Create a DB2 Table Space. Give this table space a name like MFTISTS. This table spaces should be defined as Type “Regular” and use the Buffer Pool defined in step 2. Create a DB2 Container with a unique name such as “C:\DB2Container\MFTISCTS”. This directory will be automatically created by DB2 when the table space definition is completed.
    - Create a second DB2 Table Space. Give this table space a name like MFTISTTS. This table space should be defined as Type “System Temporary” and use the Buffer Pool defined in step 2. Create a DB2 Container with a unique name such as “C:\DB2Container\MFTISCTTS”. This directory will be automatically created by DB2 when the table space definition is completed.
- If you are using an Oracle 10i or later, using Cost Based Optimization (CBO), it is strongly recommended that the optimization is tuned for first_rows for the MFT Internet Server database. To enable this, the following command should be issued from sqlplus as SYSDBA, after creating the database:

  ```
  alter system set optimizer_mode=first_rows_100;
  ```

  Warning: The DB User account used for the MFT Internet Server install must not have the DBA role assigned as this will cause the installation to fail.

3

Installing

This chapter will assist users in installing the TIBCO Software Inc.'s MFT Internet Server product. Some steps in the installation process will differ, depending on the location of your files and the platform on which you install. In this chapter, variables are indicated by *italics*, whether or not the word is in bold text. Any phrase beginning with a $ is a referenced location in your directory structure.

Installation Procedure

You must be the system Administrator of the operating system to successfully complete the MFT Internet Server installation.

Note: On Windows 2008, Windows 7, and Vista systems TIBCO recommends the built-in Administrator's account be used for the installation. If you choose to use a Windows domain user's account that has been added to the Administrators group you will need to disable User Account Control (UAC).

Note: A Java JDK (Software Development Kit) and Unrestricted Policy Files should have been installed before MFT Internet Server was installed. MFT Internet Server installation and configuration requires the *bin* directory of the JDK to be in your PATH. Instructions on how to do this are shown below.

The MFT Internet Server "install" scripts must be located in the same directory as the "cfcc.jar" file. If you are executing on a UNIX environment, make sure that the "install.sh" and "uninstall.sh" scripts have the "execute" attribute.

Java running on Windows or UNIX

1. Set the JAVA_HOME environment variable. The JDK directory name may be different in your system:
   Windows: **set JAVA_HOME=….\jdk1.7.0_51**
   UNIX: **export JAVA_HOME=…./jdk1.7.0_51**
2. Set the PATH to point to the Java\bin directory:
   Windows: **set PATH=%JAVA_HOME%\bin:%PATH%** Or
   set PATH=….\jdk1.7.0_51\bin;%PATH%
   UNIX: **export PATH=$JAVA_HOME/bin:$PATH** Or
   export PATH=…./jdk1.7.0_51/bin:$PATH
3. Verify that the path was correctly set by issuing the following command:
   Windows and UNIX: **java –version**
   java version "1.7.0_51"
   Java(TM) SE Runtime Environment (build 1.7.0_51-b13)

Note: If you intend to run the application server as a Windows Service you must set the JAVA_HOME environment variable for the System. Read Appendix C for more information.

If you are installing MFTIS on one of the supported UNIX platforms and have uploaded the files needed for installing on UNIX the default permissions should be set to the following:

cfcc.jar	-r-- r-- r--	444
EULA.txt	-r-- r-- r--	444
install-config.xml	-r-- r-- r--	444
installer.jar	-r-- r-- r--	444
install.sh	-r-x r-x r-x	555
server.jar	-r-- r-- r--	444
uninstall.sh	-r-x r-x r-x	555

Running the Automated Install

To start the MFT Internet Server automated install, type the following on the command line:

install

You will see the following:

```
                                MFT Installer Release 7.2.6
                            (supports version 7.2.1 and higher)

Please note that this install will perform multiple App Server restarts.
For this install, press the ENTER key to accept defaults and continue.

You must read the license agreement before proceeding with the installation.
Press enter to display the agreement.
```

When you press the <Enter> key you will be presented with the End User License Agreement (EULA). Press the <Enter> key as you read through each page to continue to the next page. Once you get to the last page you will be prompted to accept the license agreement. If you do not want to accept the license agreement simply type “no” and press <Enter> and the installation will end. Once the EULA is accepted the installation will continue.

Step 1: This step will extract the distribution file called cfcc.jar and setup the Java Mail if it is not already configured as well as. This step will install and configure the application server and detect the java environment variables. If you are installing on a UNIX system with IBM java you will also be presented with the question whether to put the application server in FIPS mode. When the server is put into FIPS mode, MFT will only use FIPS certified cryptographic modules when using SSL (HTTPS and FTPS), SFTP (SSH) and AS2. If you wish to change your FIPS mode configurations at a later time see section 5 for how to configure FIPS mode manually.

```
Detected Java version:  1.7.0_51.
Detected JAVA_HOME environment variable.
Using C:\Program Files\Java\jdk1.7.0_51 as path to JAVA JDK

************************************************************************
Step 1  Extracting distribution
Found distribution file c:\MFTIS\cfcc.jar
Use C:\MFTIS\cfcc.jar as the distribution? y/n [y]:
Extracting distribution file: C:\MFTIS\cfcc.jar
.........................................................................
Distribution extracted successfully!

Installing application server to C:\MFTIS\server
.................................................................................................

Using C:\MFTIS\server as path to the application server installation.
C:\MFTIS\server\conf\Catalina\localhost
```

If the OS was a UNIX system using IBM java you will be asked if you want to run in FIPS mode:

```
Using C:\MFTIS\server as path to the application server installation.

Do you wish to run in FIPS mode? y/n [n]: y
```

Step 2: This step will set up the connection to your MFT Internet Server database. For this sample install, we used Oracle as the database server. When using Oracle you must have the JDBC drivers on the system. See the Pre-requisites section of this manual for more information. (Note: For installations using a MSSQL database that uses Windows Authentication you must add the domain parameter with the domain name to the end of the database URL. To do this, type “n” when prompted with the default statement, “Use database URL:”. You will be given the opportunity to enter a new database URL to use. Copy and paste the URL that is contained in the brackets and then add a semicolon and the domain parameter at the end, (i.e., jdbc:oracle:thin:@mftdb2:1521:cfcc) and then press the <Enter> key.)

```
Step 2  Verifying database connection
Select database server type:
Enter 1 for MSSQL
Enter 2 for MySQL Enterprise Server or Community Server
Enter 3 for Oracle
Enter 4 for DB2
: 3

Oracle selected as database server type.

Enter the DNS name or IP Address of the database server...[localhost]:10.97.142.183
Enter the database port number.....................................[1521]:
Enter the database name.....................................[cfcc]:orcl
Enter the database UserID.....................................[cfcc]:
Enter the database Password.....................................[cfcc]:
Please confirm password:

The Oracle classes12.jar JDBC driver is not shipped with this product. Enter a f
ully qualified path of the driver:c:\drivers\classes12.jar

The Oracle ocrs12.jar JDBC driver is not shipped with this product. Enter a full
y qualified path of the driver:c:\drivers\ocrs12.jar

Use database URL: [jdbc:oracle:thin:@10.97.142.183:1521:orcl]? y/n [y] :

Verifying database connection using the following URL:
jdbc:oracle:thin:@10.97.142.183:1521:orcl

Successfully established connection to the database.

Start to set up pooling parameters
Select database pooling settings. Enter y to use database pooling, and n for no
pooling. [y]:

Input max active connections (positive integer). [400]:

Input max idle pool size (positive integer). [20]:

Input min idle pool size (positive integer). [10]:

Input max wait time to get a connection when there is no available connection (i
n minutes). [1]:

Input time between eviction runs to clean up pool (in minutes). [20]:

Input min evictable idle time before a connection can be removed from pool (in m
inutes). [40]:

Database pooling flag: use pooling
Max active connections: 400
Max idle pool size: 20
Min idle pool size: 10
Max wait to get a connection when there is no available connection: 1 minutes
Time between eviction runs to clean up pool: 20 minutes
Min evictable idle time before a connection can be removed from pool: 40 minutes

Use these parameters for database connection pooling? y/n [y]:
```

Step 3: Once the database connection has been established in Step 3, Step 4 will generate the MFT Internet Server database tables.

```
Step 3  Configuring the database
Executing database creation utility....
Executing database creation utility....
cmd /E:1900 /c setupdb.bat "jdbc:oracle:thin:@10.97.142.183:1521:orcl" oracle "Q
A_72" ********
Allocating DBSetup object...
Determining database version....
Installing database...
Updating database...
Updating tables...
…
…
Updating records...
```

```
Done updating database.
Successfully installed database: jdbc:oracle:thin:@10.97.142.183:1521:orcl
Successfully populated DB tables with default information.
adding URIEncoding attribute to http connector
```

If you already have a MFT Internet Server database you are advised to take a backup of the database as the MFT Internet Server install will update the existing database. You will see the following:

```
Step 3  Configuring the database
Database will be modified for new features.  Please backup database before proceeding.
Do you wish to continue? y/n [y]
```

Step 4: This step configures MFT Internet Server for SSL communications. If you do not have a certificate, then the MFT Internet Server install will create a self signed certificate. You can either use a certificate issued by a Certificate Authority (CA) or use a self signed certificate. During the process you will have the opportunity to choose the signature algorithm that will be used to sign the self-signed certificate, the highest strength being SHA512 with RSA and the lowest being SHA1 with DSA. If you are unsure what should be used in your environment choose the default setting of SHA1 with RSA.

Note:

- Self signed certificates are only practical for testing purposes but do allow you to get up and running quickly while you wait for an external CA to sign a certificate for you.
- Assigning port numbers below 1024 (so-called 'low numbered' ports) can only be bound to by root on UNIX systems.

```
Step 4  Evaluating the application sever installation for HTTPS connectors
Reading the application server configuration file: C:\MFTIS\server\conf\server
xml
Found no pre-existing HTTPS connectors!
Do you have a pre-exisiting Java Keystore to be used as a server key for SSL co
munication? y/n/? [n]:

Creating keystore for SSL communication
Enter the keystore path and filename..[C:\MFTIS\keystore\keystore.jks]:
Directory C:\MFTIS\keystore does not exist! Create? y/n [y]:
Enter the keystore password (at least 6 characters)..[changeit]:
 Enter the alias of your private key.....................[cfcc]:
Enter the DNS Name or IP Address of your server.....:10.97.142.191
Select the signature and key algorithms you wish to use........:
1. SHA1 with RSA
2. SHA256 with RSA
3. SHA384 with RSA
4. SHA512 with RSA
5. SHA1 with DSA
Please enter your selection. [1]: 4
Enter your Company Name.............................[Optional]:TIBCO
Enter your Organizational Unit Name.................[Optional]:Web Debt
Enter the City where your company is located.........[Optional]:Palo Alto
Enter the State where your company is located........[Optional]:CA
Enter the two-letter country code for this unit......[Optional]:US

Keystore filename    : C:\MFTIS\keystore\keystore.jks
Keystore password    : ********
Key alias            : cfcc
Server address       : 10.97.142.191
Signature and key alg: SHA512withRSA
Organization         : TIBCO
Organizational Unit  : Web Debt
Locality             : Palo Alto
State                : CA
Country              : US
Create a keystore with the above information? y/n [y]:

Creating keystore......
C:\Program Files\Java\jdk1.6.0_29\bin\keytool -genkey -keystore C:\MFTIS\keys
ore\keystore.jks -storepass ******** -keypass ******** -keyalg RSA -sigalg SHA5
2withRSA -alias cfcc -keySize 2048 -validity 3650 -dname CN=10.97.142.191, O=TI
CO, OU=Web Dept, L=Palo Alto, ST=CA, C=US

Enter the HTTPS Port to listen for connections… [443]:
```

Step 5:This step will configure the MFT Internet Server components and ports on the application server. The AJP port is used for forwarding requests from an HTTP server.

```
Step 5  Updating the application server Connector Configuration

Default HTTPS Connector parameters for port 443:
The Default Verbosity Level                    - 2
The Default Debug Level                        - 2
The Default Buffer size                        - 2048
The Default Connection Timeout                 - 60000
The Default DNS Lookup set to                  - true
The Default Max active requests                - 128
The Default Min Processors                     - 5
The Default Max Processors                     - 100

Accept these parameters? y/n [y]:

Enter the HTTP port to listen for connections... [80] :

Enter the port to listen for shutdown requests... [7005] :

Enter the AJP port... [7009] :
```

Step 6: This step will configure the context root that will be used in the URL. The context name should be set to an alphanumeric name. Using special characters within a context name can cause unpredictable results.

```
Step 6  Evaluating the application server installation for contexts
Enter the context root for this installation ........[cfcc]

Reading context configuration file: C:\MFTIS\server\conf\Catalina\localhost\cfcc.xml
Found no pre-existing Contexts
```

Note: If you are upgrading you will be prompted to backup your present settings as only one instance of cfcc can exist on the server.

Step 7: This step will extract the cfcc.war file in order to install the MFT Internet Server application.

```
Step 7  Installing web application
Use C:\MFTIS\server\webapps\cfcc as the installation directory? y/n/? [y]:

Extracting distribution\cfcc.war to C:\MFTIS\server\webapps\cfcc
```

Step 8: This step will verify the context configuration for MFT Internet Server.

```
Step 8  Updating the application server context configuration

Default Context parameters:
The Default Log File Prefix                    - localhost_cfcc_
The Default Log File Suffix                    - .txt
The Default Log File Timestamp                 - true
The Default Log File Verbosity Level           - 2
The Default Log File Debug Level               - 0

Add a new context with the above parameters? y/n/? [y]:
```

Step 9: This step will update the MFT Internet Server (MFTIS) web.xml file on the local host. You will also be asked if you want to install the Administrator service (Administration web pages) for the MFT Internet Server. This should only be installed inside your internal network. When MFT Internet Server shares a database with an MFT Command Center installation all Administration for the MFT Internet Server can be performed from the MFT Command Center Administrator web pages. If this is the desired configuration for your environment, answer “n” (No) to this question.

```
Step 9 Configuring web.xml
```

```
Enter the name of the host on which the application will run. [SystemA]:

Administrator service is used to manage the application.
You should only install this service inside your internal network.
Install this service? y/n? [y]:

Enter a directory to store log files......[c:\MFTIS\logs]:

Configure web.xml with the above parameters? y/n [y]:
Starting the application server.................. [OK]
```

Step 10: This step will deploy the MFT Internet Server web service.

```
Step 10 Deploying services
Executing deploy command.
Cmd /E:1900 /c deploy.bat 127.0.0.1 80 admin ****** cfcc
This may take a few moments......
```

Step 11: This step will generate the SOAP stubs MFT Internet Server will use.

```
Step 11 Generating SOAP Stubs
Executing genstubs command.
Cmd /E:1900 /c genstubs.sh 10.97.142.191 8080 admin ******** cfcc http
This may take a few moments......
```

Step 12: This step will install the stubs generated for the MFT Internet Server web service in Step 12.

```
Step 12 Installing SOAP Stubs
Executing installstubs command.
Cmd /E:1900 /c installstubs.sh c:\MFTIS\server\webapps\cfcc
This may take a few moments......
```

Step 13: This step is to verify you have installed the required AES encryption policy files needed for MFT Internet Server. If you have not already installed the policy files please refer to the Pre-requisites section to read about how to obtain the files you need. If your policy files have been installed you will not see the first half of this message as seen below.

```
Step 13 Installing AES encryption library
In order to use 256 bit secure keys you must download the JCE Unlimited Strength Jurisdiction
Policy Files from http://java.sun.com. After downloading, unzip the zip file to
/usr/java6_64/jre/lib/security.

Please disregard the above message if you have already installed the policy files.

Your Java Runtime Environment (JRE) must be upgraded to support AES encryption.
Proceed with the upgrade (recommended)? y/n/? [y]:

Restarting the application server
Stopping the application server.............................. [OK]
Starting the application server.............................. [OK]
```

Step 14: When MFT Internet Server shares a database with MFT Command Center, transfers among other supported features can be performed to/from JMS Queues. To use JMS in conjunction with MFT Internet Server you must copy the JMS jar files for your JMS Server installation to the <MFTIS_install>WEB-INF\libs directory as noted in the message that will be displayed. The jar files used must be the same JMS jar files that MFT Command Center install is configured with.

```
Step 16 Copy JMS files

If you are using the JMS interface, you must copy the JMS jar files to the
following location:
C:\MFTIS\server\webapps\cfcc\WEB-INF\lib
These jar files are typically found in the JMS Server installation.
Restart the MFT server after copying the jar files.
You can configure and test the JMS settings through the Command Center.
Go to the Management > Manage Services > Configure JMS Service page.
```

```
On that page you can click on help for a list of the provider specific jar files.

Press the enter key to continue.

Installation completed!  Details are in the install.log file.
```

The MFT Internet Server automated install is complete.

If you are installing MFT Internet Server on a Windows system a Java window labeled MFT Server will display during and after a successful installation. This window must be kept opened in order for the MFT Internet Server to continue running. Closing the MFT Server window will shutdown the web application.

You may stop and start the MFT Server by running the **startup** and **shutdown** scripts for the appropriate system in the server directory at: <MFTIS_Install>/server/bin

Once MFT Internet Server is installed successfully, it is time to access the Internet Server web pages. The MFT Internet Server is accessed using one of the following URLs:

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

Note: If the default context was not used during installation, the redirector file for this shortcut as well as others mentioned later in this manual will need to be updated to redirect to the non standard context. Follow the instructions below to make these changes:
The redirection files can be found in the <MFTIS_Install>\server\webapps\ROOT directory. Use a text editor to open and change the “cfcc” context in these files to the new context chosen during the install. Once your changes have been made save and close the files.

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.

Next see Chapter 5, *Software License Keys.*

4

Upgrading

This chapter will assist users upgrading from MFT Internet Server versions 6.5.1 and greater as well as instruct the Administrator what is needed when upgrading the Java JDK. Some steps in the upgrading process will differ, depending on the version of the former MFT Internet Server you have installed presently. In this chapter, variables are indicated by *italics*, whether or not the word is in bold text.

In a continued effort to clearly delineate the features supported by the Command Center and Internet Server, the Command Center and Internet Server installations have been separated. The new streamlined installation process designed specifically for each component eliminates any potential confusion that was caused by the installation procedures of the past. The Command Center is the centralized administrative interface that allows you to manage and control MFT Platform Server functions, Alerts, audit Collections, Status Service and Integrates JMS functionality. The Internet Server is the component that provides connectivity to remote systems using open file transfer protocols. Both the Command Center and Internet Server come with an Administrative interface that allows for configuration and management. In installations where there will be a Command Center sharing the same database as an Internet Server there is no need to install the standalone Internet Server Administrative Service; all functions that are available in this service are available in the Command Center.

If you are currently running v6.5.1 – v7.1.1 Command Center/Internet Server on the same server sharing a database the same setup can be done as long as different ports are used. By default Command Center v7.2.6 uses ports 8080 and 8443 for http and https and Internet Server v7.2.6 uses ports 80 and 443 for http and https respectively.

MFT Internet Server Upgrade

When upgrading from release level 6.5.1 and 6.7 you will no longer need your web application server. MFT Internet Server and Internet Server come complete with an internal application server. If your environment is also configured using LDAP sync please contact our TIBCO Technical Support team for further instructions on this upgrade process.

6.5.1 And 6.7 Upgrades

For those upgrading from release level 6.5.1 and 6.7 please follow the instructions below:

Step 1) Stop the Web Server.
Step 2) Backup your MFT database.
Step 3) Backup your `<MFTIS_Install>` installation directory.
Step 4) Backup your entire Web Server environment.
Step 5) Open a Command Prompt window and navigate to your `<MFTIS_Install>` installation directory and run the command, **uninstall**.

Step 6) Download and have available on the installation server the supported database driver(s) needed as per the instructions found in the Pre-requisites section of this manual. As per release MFTIS v7.1 these drivers are no longer shipped.

Step 7) Due to supporting JDK 5 through 7 the following file(s) must be deleted before running the installation: <JAVA_HOME>/jre/lib/ext/bcprov*.jar
If you do not complete this step you will see something like the following during the install at Step 14:

```
Step 14 Installing AES encryption library
…
…
…
Please make sure that file
/usr/lib64/jvm/java-1.6.0-openjdk-1.6.0/jre/lib/ext/bcprov-jdk16-138.jar
is DELETED or MOVED to another directory.

NOTE: You may have to stop your application server to delete this file.
      Please make sure that you restart the server before continuing.

Press ENTER when complete.....................
```

Step 8) Follow the installation instructions found in the Running Automated Install section of this manual.

Note: During the installation you will be asked if you have a pre-existing keystore. Make note of your pre-existing keystore and be prepared to enter the private key password.

Note: If the pre-existing web server contains other applications running and you want to install MFT Internet Server on the same machine you will need to set different HTTPS, HTTP, and AJP ports for MFT Internet Server to use to avoid any port conflicts with your web server.

Step 9) When the product installs on a Windows server it will run as an application. If you would like the MFT Server to run as a service see the section called Auto Start on Boot-up of this manual.

Step 10) Database keys are no longer needed for the MFT Internet Server. If one is displayed in the Manage License Keys web page it should be deleted.

Upgrades from 7.2.0

For those that are upgrading from release level 7.2.0 a full installation must be done. Please follow the instructions found in the Installation Procedure section of this manual.

7.2.1 And Above Upgrades

For those that are upgrading from release level 7.2.1 and above please follow the instructions below.

Note: You will need the Administrator user name and password.

Step 1) Stop the application server.
Step 2) Backup your <MFTIS_Install> installation directory.
Step 3) Backup your MFT database.
Step 4) From the present <MFTCC_Install> directory copy and replace the old installer.jar file with the new **installer.jar** and copy and paste the new **SPMFT726.jar**.

Note: You can run an entire new install from a new directory by coping all the v7.2.6 files however you will need to run some addition steps.

a) During the installation you will be asked if you have a pre-existing keystore. If you want to use this pre-existing keystore make note of the full path and be prepared to enter the private key password.
b) If you are running on a Windows platform and have installed the Auto Start program you will need to remove the service from the old installation directory and reinstall it from the new installation directory. See Appendix C for instructions.

c) You will need to download the supported database driver(s) needed as per the instructions found in the Pre-requisites section of this manual. As per release MFTCC/IS v7.1.1 these drivers are no longer shipped.

d) Due to supporting JDK 7 the following file(s) must be deleted before running the installation: <JAVA_HOME>/jre/lib/ext/bcprov*.jar. If you do not complete this step you will see the following during the install at Step 14:

```
Step 14 Installing AES encryption library
…
…
…
Please make sure that file
/usr/lib64/jvm/java-1.6.0-openjdk-1.6.0/jre/lib/ext/bcprov-jdk16-138.jar
is DELETED or MOVED to another directory.

NOTE: You may have to stop your application server to delete this file.
      Please make sure that you restart the server before continuing.

Press ENTER when complete.....................
```

e) Follow the installation instructions found in the Running Automated Install section of this manual.

f) If you are running on a Windows platform. You can install the Auto Start program at this time from the new installation directory. See Appendix C for instructions.

Step 5) Run the following command on Windows: **install SPMFT725** on UNIX run: **install.sh SPMFT725**.

Note: You will be asked to stop and start the application many times through the upgrade

Note: If the pre-existing web server contains other applications running and you want to install MFT Internet Server on the same machine you will need to set different HTTPS, HTTP, and AJP ports for MFT Internet Server to use to avoid any port conflicts with your web server.

Step 6) Database keys are no longer needed for the MFT Internet Server. If one is displayed in the Manage License Keys web page it should be deleted.

Java JDK Upgrade

When upgrading the Java JDK that is being used by MFT Internet Server you will need to update a few items before the Internet Server will start to use the new Java JDK.

1. If MFT Internet Server is running on a Windows system and is running as a service, stop the MFT Internet Server service.
2. Go to <MFT_Install>\server\bin directory and run the following command and answer the question(s) to uninstall the service:
   service remove
3. Update the JAVA_HOME environment variable on the system to point to the new JDK directory. Then verify the system is pointing to the new Java JDK run the following command to verify the version:
   java –version
4. Update the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. For more details see the pre-requisites for Java of this manual.
5. From the <MFT_Install>\distribution\crypto directory copy files **bcprov-jdk15on-147.jar** and **bcprov-ext-jdk15on-147.jar** to the following <JAVA_HOME>\jre\lib\ext director.
6. From the <MFT_Install>\distribution\crypto directory copy file **bcpg-jdk15on-147.jar** to <MFT_Install>\server\webapps\<context>\WEB-INF\lib directory.
7. Backup the file **java.security** found in the following directory <JAVA_HOME>\jre\lib\security.
8. Open the file **java.security** using notepad on Windows or vi editor on UNIX. Scroll down until you see the comment "# List of providers and their preference orders (see above)". Add the following security provider if you do not see it in the list at position 3 and reorder the other security providers as necessary:

security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider

9. If MFT Internet Server is installed on a Windows system you can now go to <MFTCC_Install>\server\bin directory and run the following command and answer the question(s) to install MFT to run as a service:
   service install
10. Start MFT Internet Server.

5

Software License Key

MFT Internet Server requires a software license key to operate. The product comes with a 60 day temporary key.

The license key used by the MFT Internet Server application is:

- The MFT Internet Server Key is installed on each server that will be running the MFT Internet Server application. This key is tied to the host name of the server hosting the MFT Internet Server application. If there are multiple machines that will be hosting instances of MFT Internet Server, each one of these machines must have a license key.

Applying the Software License Key

MFT has two types of License keys that can be applied, a Command Center license or an Internet Server license. 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 a permanent license key, 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 of Internet Server, and License Key information in the fields provided:

- Server Name: Cut and paste the Server Host Name used during the install. This can be found on the **Administration > License > Host Information** web page.
- Server Type: Select the type of **Internet Server**.
- License Key: Paste in the license key that is affiliated with the Server Name field above. 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.

Note: If MFT Command Center is Administrating MFT Internet Server and the MFT Internet Server Administrator service was not installed the license key must be applied from the MFT Command Center Administrator web pages. 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.

6

FIPS 140-2 Manual Configuration

This section will guide you through the required configuration steps to enable MFT Internet Server's FIPS 140-2 compliant processing. These steps are only necessary if you did not enable FIPS mode during installation. If you enabled FIPS mode during installation, the installer automatically configured FIPS mode and no further action is necessary.

Enable FIPS Mode Manually

There are four steps necessary to put MFT into FIPS mode, but your environment must support FIPS mode in order to enable it. See the pre-requisites sections for FIPS mode requirements. Each step is detailed in the sections that follow.

1. Set your Browser to use TLS.
2. Set IBM Java security to use the FIPS certified cryptographic security provider.
3. Set the MFT Internet Server/Internet Server environment variable.

Step 1: Setting your Browser to use TLS.

All browsers used to access MFT Internet Server must be set to use TLS (Transport Layer Security) to make a secure connection and login after putting the application server into FIPS mode. TLS can be enabled by performing the following steps:

1) Open your browser and click the Tools menu and click on Internet Options
2) Now click on the Advanced tab.
3) Scroll down to the Security section in the list and look for a check box with the words "Use TLS x.x", (x.x stands for a version number). Enable this option.
4) Click Ok and refresh your page.
5) You should now be able to login to your MFT Internet Server.

Step 2: Set the IBM Java security to use the FIPS certified cryptographic security provider.

You must set the IBM security file by performing the following steps:

1) Stop the application server. *Note: For information on starting and stopping the application server please go to the end of Section 3.*
2) Go to your <JAVA_HOME>\jre\lib\security directory and open your java.security file with any available text editor.

3) Uncomment the following value by removing the pound sign (#) from the front of the statement (If you do not see the statement shown below in your file, you must add it to the top of the list as number 1):

```
#security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
```

4) Reset the security provider number values for the other security providers so they are in number order from 1 through 11.

5) When you are done editing the file, save your changes and exit the file.

6) Now navigate to the following directory: <MFTIS_Install>/server/webapps/<CONTEXT_NAME>/WEB-INF/ and open the web.xml file to edit using an available text editor.

7) Search for the SSHSecurityProvider parameter and configure it as follows:

```
<context-param>
   <param-name>SSHSecurityProvider</param-name>
   <param-value>com.ibm.crypto.fips.provider.IBMJCEFIPS</param-value>
</context-param>
```

8) When you have finished, save the file.

9) Do not start the application server yet, go to Step 3.

Step 3: Set the MFT Internet Server environment variable.

The setenv.sh file is located in the <MFTIS_Install>/server/bin directory. This script sets environment variables needed by the MFT server.

The file should look like the following:

```
#!/bin/sh
CATALINA_OPTS="-Xms512m -Xmx1024m"
FIPS_MODE="false"
```

Change the value to read FIPS_MODE="true". When you are done, save and exit the file.

Start your application server.

MFT Internet Server will now operate in FIPS mode.

Taking the MFT server out of FIPS mode

The following describes how to manually take the MFT server out of FIPS mode if you have enabled it.

There are four steps necessary to take MFT out of FIPS mode.

1. Remove FIPS certified cryptographic provider from the list of providers in the java.security file.
2. Set the MFT environment variable FIPS_MODE to false in the setenv.sh file.
3. Remove the provider name from SSHSecurityProvider parameter in the web.xml file.
4. Restart the server.

If you manually enabled FIPS mode you will have to undo the changes you made when putting MFT into FIPS mode. If FIPS was automatically configured during installation, see the section “Configure FIPS mode Manually” for more details on which files to edit.
NOTE: When removing the cryptographic provider from the **java.security** file you can either comment out the line with the # sign or delete the line. You must fix the order of the providers after that.

7

Changing the Default Logos

There are four logos within MFT Internet Server that can be customized.

Used by MFTIS Thin Client: file **ft_logo.gif** size 245x89

Used by MFTIS Administrator login: file **corporate_logo.png** size 95x30

Used by MFTIS Administrator login help pages: file **mft_logo.png** size 268x64

Used by MFTIS Administrator: file **mft-is-logo.png** size 204x88

Shown in the upper left corner of your browser

Used by MFTIS Administrator login: file **product_logo_is.png** size 663x144

Used by MFTIS Administrator and Thin Client: file **tibco-logo-117-24.jpg** size 117x24

Internet Server Desktop Client Images:

Used by Desktop Client: file **about-company-logo.png** size 74x74

Please follow these steps for customizing MFT Internet Server/Internet Server logos:

1. Navigate to <MFTIS_Install>\server\webapps\cfcc\view\images directory.
2. Rename the logo that is being replaced by adding .OLD after the file extension (e.g., logo.png.old).
3. Copy your new logos into the directory and make sure the file names, type, and sizes MUST match the original file names in the directory.
4. Refresh your browser.

8

Uninstall

To uninstall MFT Internet Server you would use the **uninstall.bat** program for Windows installations or **uninstall.sh** program for UNIX installations located in your <MFTIS_Install> directory.

Note: If MFT Internet Server have been installed as a Windows service it should be removed before running the uninstall.bat. Please see the Remove Windows Auto Start section in this manual to remove the service.

From the command line run the following command on either Windows or UNIX:

uninstall

You will see the following:

```
uninstall

Please note that this uninstall will perform multiple App Server restarts.
For this uninstall, press the ENTER key to accept defaults and continue.

Stopping the application server.............................[OK]

Uninstalling the application server HTTPS connector...........

Uninstalling context......
Deleted distribution directory.

Uninstallation completed! Details are in the uninstall.log file.
```

Your MFT Internet Server uninstall is complete.

A

Appendix A. Worksheet

This worksheet is designed to allow you to have one convenient location to collect information that will be used throughout the installation and configuration of the MFT Internet Server.

A.1 Install Worksheet

This worksheet is provided to gather information prior to the install of MFT Internet Server. The user may also use the defaults provided by the installation program.

Web Server Information:

1. Have you downloaded and installed the Sun/IBM Java JDK _____

4. Is the JAVA_HOME variable set: _____

5. Have you downloaded and installed the Java AES encryption policy files: _____

Database Information:

6. What is the DNS or IP Address and port number for the MFT Internet Server database: _____

7. What database admin id and password should be used: _____

Java Keystore Information: (This information is optional because MFT Internet Server will create one if one is not provided)

8. What is the path and file name of your java keystore: _____

9. What is your keystore password: _____

10. What is the Alias for the private key: _____

MFT Internet Server Application Information:

11. What is the DNS or IP Address of the server where MFT Internet Server application is being installed? _____

12. What context root do you want to use (default is cfcc): _____

13. In what directory should log files be kept (defaults to install directory): _____

LDAP Information: (This information is optional because you may not be using LDAP for authentication.)

14. LDAP server type: _____

15. DNS or IP Address of the LDAP server: _____

16. What is the LDAP port number: _____

17. What is the LDAP Administrator DN: _____

18. What is the password for the User DN: _____

B

Appendix B. Certificate Update Procedure

MFT Internet Server uses two types of certificates:

A. HTTPS Certificate used for communicating with MFT Internet Server using HTTPS (HTTP over SSL)
B. Applet Certificate used to sign the JAVA applets used by MFT Internet Server to transfer files

This document defines the procedures used to generate and use both type of certificates.

Note that it is best to create a new keystore for each type of certificate and most Certificate Authorities (CA) require separate certificates for HTTPS and Applet signing. You must purchase the correct certificates.

B.1 HTTPS Certificate Update Procedure

In order to obtain a new HTTPS certificate from the CA, a certificate request must be issued. Please record all steps executed and their output into a file called “cert.https.log” for tracking.

Note: 1) The commands listed here are only examples and do not include all the options that the keytool program offers. Careful consideration should be taken when generating your key pair for your environment. Consult with your Web Administrator.

2) Each certificate requires a separate keystore.

3) The CA may have specific options required for creating an HTTPS certificate. Review the instructions provided by the CA before generating the certificate request.

1. To generate a Java keystore and key pair where the certificate would be considered valid for 365 days you could issue the following example command:

```
keytool –genkey –v –alias cfcc –keyalg RSA –keysize 2048 –keypass
changeit –keystore <MFT_Install>\keystore\newkeystore.jks -storepass
changeit –validity 365
```

The keytool utility will then display messages requesting more information about the certificate request. The most important information to enter is when the keytool utility asks “What is your first and last name”. You must enter the DNS name that is used to access MFT Internet Server/Internet Server. This is used as the CN (Common Name) in the certificate; HTTPS requires the CN to match the DNS name used to access the HTTPS Server.

Example: `mft.yourcompany.com`

Notice in the example command above the keypass and storepass are the same. These two passwords must match each other. We suggest using the same keystore/storepass password that was used to create the original keystore. This way you will not have to update the keystore password in the product configuration files.

2. Generate a Certificate Request

```
keytool –v –certreq –alias cfcc –file <MFT_Install>\keystore\cfcc.csr –
keypass changeit –keystore <MFT_Install>\keystore\newkeystore.jks -
storepass changeit
```

3. Submit the Cert Request File created in the above command to the CA.

4. Install the CA Certificate into the Internet Server’s keystore:

: Save the Certificate returned by the CA to a file <Cert File>
: Execute the keytool command to import the certificate

```
keytool –v –import –alias cfcc -trustcacerts –file <Cert File> -
keystore <Keystore File Name>
```

NOTE: Some CAs now issue an intermediate certificate along with the main certificate. If this is true for your CA, then import certificates using unique aliases to the keystore created in Step 1. This step is required to prevent the client from receiving a certificate warning.

5. Update the MFT Server to use the new Keystore:

   Note: You could rename your old keystore file for example org.keystore.jks and then rename the new keystore to have the old file name in the same location and then no changes are needed to the server.xml and you can go to Step 6.

   Change the Keystore path of the file located at: <MFTIS_Install>\server\conf\server.xml
   : Look for the Connector associated with the HTTPS port
   : Update the “keystoreFile” parameter to point to the new keystore
   : If the password has changed, update the “keystorePass” parameter with the new keystore password.

6. Stop and Start the MFT Internet Server.

7. Verify that the MFT Server is listening on the defined port.

8. Perform a file transfer to verify the Internet Server is functioning correctly.

B.2 Applet Certificate Update Procedure

A separate JAVA applet certificate is required to sign the MFT Internet Server Transfer applet. Most Certificate Authorities (CA) require separate certificates for HTTPS and Applet signing. You must purchase the correct type of certificate. In order to obtain a new applet certificate from the CA, a certificate request must be issued. Please record all steps executed and their output into a file called "cert.applet.log" for tracking.

Note: 1) The commands listed here are only examples and do not include all the options that the keytool program offers. Careful consideration should be taken when generating your key pair for your environment. Consult with your Web Administrator.

2) Each certificate requires a separate keystore.

3) The CA may have specific options required for creating an HTTPS certificate. Review the instructions provided by the CA before generating the certificate request.

1. To generate a Java keystore and key pair where the certificate would be considered valid for 365 days you could issue the following command:

```
keytool –genkey –v –alias cfcc –keyalg RSA –keysize 2048 –keypass
changeit –keystore <MFT_Install>\keystore\newkeystore.jks -storepass
changeit –validity 365
```

The keytool utility will then display messages requesting more information about the certificate request. The most important information to enter is when the keytool utility asks "What is your first and last name". You must enter the DNS name that is used to access MFT Internet Server/Internet Server. This is used as the CN (Common Name) in the certificate; HTTPS requires the CN to match the DNS name used to access the HTTPS Server.

Example: `mft.yourcompany.com`

Notice in the example command above the keypass and storepass are the same. These two passwords must match each other. We suggest using the same keystore/storepass password that was used to create the original keystore. This way you will not have to update the keystore password in the product configuration files.

2. Generate a Certificate Request

```
keytool –v –certreq –alias cfcc –file <MFT_Install>\keystore\cfcc.csr –
keypass changeit –keystore <MFT_Install>\keystore\newkeystore.jks -
storepass changeit
```

3. Submit the Cert Request File created in the above command to the CA.

4. Install the CA Certificate into the Internet Server's keystore:

: Save the Certificate returned by the CA to a file <Cert File>
: Execute the keytool command to import the certificate

```
keytool –v –import –alias cfcc -trustcacerts –file <Cert File> -
keystore <Keystore File Name>
```

NOTE: Some CAs now issue an intermediate certificate along with the main certificate. If this is true for your CA, then import certificates using unique aliases to the keystore created in Step 1. This step is required to prevent the client from receiving a certificate warning.

5. Install the Applet certificate into the keystore

   : Save the Certificate returned by the CA to a file <Cert File>
   : Execute the keytool command to import the certificate

   ```
   keytool –v –import –alias cfcc -trustcacerts –file <Cert File> -
   keystore <Keystore File Name>
   ```

6. Sign the JAVA Applets
   Run the following from the <MFTIS_Install>\distribution\setup directory

   Note: You can also use the same signjar command that was used in the Internet Server install (install.log) as your example.

   ```
   signjars.bat [javakeystore] [keystore password] [keystore alias] [path to
   the MFT cfcc directory]
   ```

   - java keystore: This is the name of the java keystore to be used for signing.
     Note: This applet certificate should be in a different keystore than the HTTPS certificate. If the keystore location contains spaces, enclose it in quotes.
   - keystore password: This is the password for the keystore.
   - keystore alias: This is the alias for the key to be used.
   - path to cfcc directory: This is the path to the MFT Internet Server's cfcc web context <MFTIS_Install>\server\webapps\cfcc. If the directory contains spaces, enclose it in quotes.

   Note: The permissions for the UNIX signjars script must be changed so that it has execute rights.

   It is recommended that you use the same alias as you used in the self-signed step (default value is cfcc, but reference the install.log to verify) in order to ensure there is only one signature per jar.

7. Stop and Start the MFT Server.

8. Perform a file transfer. Verify that the certificate associated with the File Transfer Applet points to the new certificate. Note that you may need to clear your browser cache to see the new certificate.

C

Appendix C. Auto Start on Boot-up

By default the application server is not configured to automatically start on boot-up. This section describes how to setup an automatic start for the MFT Internet Server 7.2.2 embedded application server on a UNIX/Linux or Windows systems.

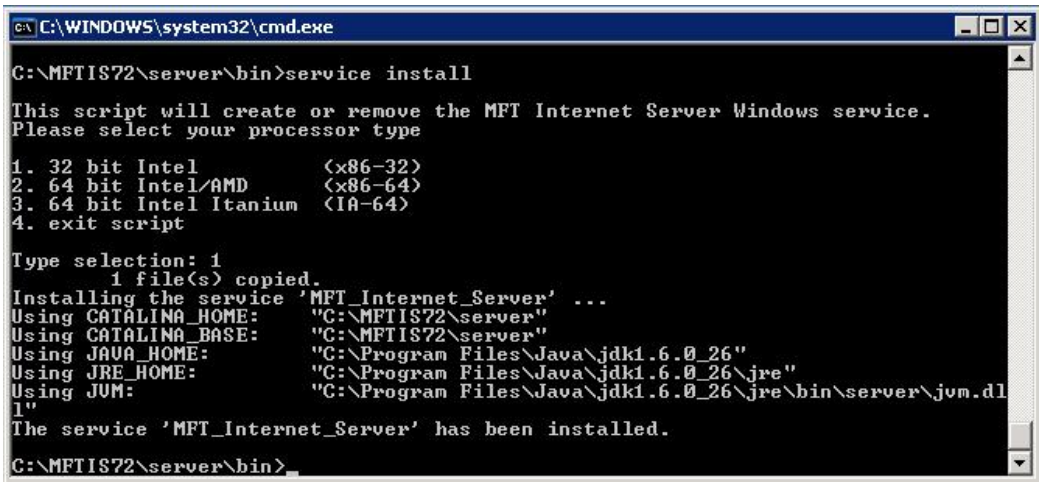
C.1 Windows Systems

First check the JAVA_HOME System environment variable has been configured on your server. To set the variable open your System Properties window and click on the Advanced Tab. Click on the button with the name *Environment Variables* on it. In the bottom window labeled, System variables, search for the JAVA_HOME variable. If you do not see it in the list you must add the JAVA_HOME variable pointing to your Java's jdk file. For example: C:\Program Files\Java\jdk1.7.0_516. *Note: If you created a new variable you must restart the system before the new variable will be recognized.*

Next navigate to the <MFTIS_Install>\server\bin directory and stop your present MFT Internet Server application using the shutdown command. Once the server has stopped run the following install command from the same directory:

service install

You will be prompted to choose which processor you are currently running with as seen in the example screenshot below:



Once the script has completed running you can now open your services window and see the MFT Internet Server service listed as seen below:

Note: The MFT Internet Server service is installed by default using the **Manual** startup option. To configure the service to start up automatically when you restart Windows right-click **MFT Internet Server** in the Windows Services console and click **Properties**. Set **Startup Type** to **Automatic** and click **OK**.

C.2 UNIX/Linux Systems

There are a number of methods that different UNIX/Linux operating systems use to automatically start processes at boot time. This example has been developed specifically for the Red Hat Linux Enterprise operating system, but has been tested successfully on many other UNIX and Linux distributions. The instructions for setting auto start on Red Hat Linux are:

In order to have the MFT Internet Server automatically start on boot-up, first add the JAVA_HOME variable to the <MFTIS_Install>/server/bin/setenv.sh file:

```
CATALINA_OPTS="-Xms512m -Xmx1024m"
JAVA_OPTS="-Duser.language=en -Duser.country=US"
JAVA_HOME="/opt/jdk1.7.0_03"
```

Then add the startup.sh shell script to the /etc/rc.local file.

For example: /opt/MFTIS/server/bin/startup.sh

C.3 Remove Windows Auto Start Settings

Should you want to remove the auto start feature simply stop the MFT Internet Server service and navigate to the <MFTIS_Install>\server\bin directory and run the following command:

service remove

The following message will be displayed:

The service 'MFT_Internet_Server' has been removed

D

Appendix D. Setting Ciphers and Hashes

D.1 FTP and SFTP Ciphers and Hashes

MFT Internet Server's SSH and FTP components support several different encryption algorithms (i.e., ciphers). You can optionally restrict the ciphers MFT Internet Server will support, if desired, by modifying MFT Internet Server's web.xml file.

1) To view a list of the ciphers MFT Internet Server will support in your environment, navigate to your web server's standard out log, **stdout.log** located in the `<MFTIS_Install>`/server/logs directory and perform the following steps, *Note: On Windows installations that have not setup the Auto Start the standard out messages will be written to your MFT Server command prompt window being used as your console. If you are using a UNIX system the message will be written to the catalina.out log*:
    a. Start the MFT FTP and/or SSH servers if they are not already running. *Note: For information on starting and stopping the MFT FTP/SSH servers please see the MFT Internet Server User Guide.*
    b. Go to your web server standard output log and open it with any available text editor.
    c. Search for one of the following text strings:
        i. FTP Server – supported ciphers
        ii. SSH Server – supported ciphers
        iii. SSH Server – supported hash

2) By default, MFT Internet Server supports all ciphers contained in the log file. Once you have viewed the supported ciphers listed in your log file you can limit which ciphers or hash algorithms that will be used by MFT Internet Server by performing the following steps:
    a. Stop your application server.
    b. Navigate to the following directory: `<MFTIS_Install>`/server/webapps/cfcc/WEB-INF/
    c. Open the web.xml to edit using any available text editor.
    d. At the top of the file you will see the following parameters sections:

```
<context-param>
        <param-name>FTPCipherSuite</param-name>
        <param-value/>
</context-param>

<context-param>
        <param-name>SSHCipherSuite</param-name>
```

```
        <param-value/>
</context-param>

<context-param>
        <param-name>SSHDigestSuite</param-name>
        <param-value/>
</context-param>
```

The following example limits the ciphers and hash algorithms that will be used by MFT Internet Server (multiple ciphers and hash algorithms can defined by separating each ciphers or hash algorithms with a comma):

```
<context-param>
        <param-name>FTPCipherSuite</param-name>
        <param-value>SSL_RSA_WITH_AES_128_CBC_SHA,
     SSL_RSA_WITH_AES_256_CBC_SHA</param-value>
</context-param>

<context-param>
        <param-name>SSHCipherSuite</param-name>
        <param-value>aes192-cbc,aes256-cbc</param-value>
</context-param>

<context-param>
        <param-name>SSHDigestSuite</param-name>
        <param-value>hmac-sha1</param-value>
</context-param>
```

Restart your application server.

D.2 HTTP SSL Ciphers

For an increased level of HTTP SSL security in MFT Internet Server (MFTIS), running the server in FIPS mode is recommended. If you do not have your MFTIS server running in FIPS mode however, and higher HTTP SSL cipher strengths are required for client connections, you can edit the following MFT configuration file to enforce certain SSL ciphers.

```
<MFTIS_Install>/server/conf/server.xml
```

Within this file is a default HTTP connector, as seen in our example below:

```
<Connector SSLEnabled="true" acceptCount="128" bufferSize="2048"
clientAuth="false" compression="off" connectionLinger="-1"
connectionTimeout="60000" debug="2" disableUploadTimeout="true"
enableLookups="true" keystoreFile="C:\Program
Files\TIBCO\MFTIS1\keystore\keystore.jks" keystorePass="changeit"
keystoreType="JKS" maxKeepAliveRequests="100" maxProcessors="100"
maxThreads="150" minProcessors="5" port="443"
protocol="org.apache.coyote.http11.Http11Protocol" proxyPort="0"
redirectPort="-1" scheme="https" secure="true" sslProtocol="TLS"
tcpNoDelay="true" useURIValidationHack="true"/>
```

The list of available ciphers can be found by following D.1 section 1.

Below is an example that will force client connections to maintain cipher strengths of 128bit or greater. *Note: The ciphers in this example are from Oracle Java 6 update 26*:

```
ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
```

Below is another example that will force client connections to maintain cipher strengths of 256bit or greater *Note: Only certain browsers will support 256bit cipher strength. The ciphers in this example are from Oracle Java 6 update 26:*

```
ciphers="TLS_RSA_WITH_AES_256_CBC_SHA"
```

We have taken the example above and placed it in our default Connector to show how this would be added:

```
<Connector SSLEnabled="true" acceptCount="128" bufferSize="2048"
clientAuth="false" compression="off" connectionLinger="-1"
connectionTimeout="60000" debug="2" disableUploadTimeout="true"
enableLookups="true" keystoreFile="C:\Program
Files\TIBCO\MFTIS\keystore\keystore.jks" keystorePass="changeit"
keystoreType="JKS" maxKeepAliveRequests="100" maxProcessors="100"
maxThreads="150" minProcessors="5" port="443"
protocol="org.apache.coyote.http11.Http11Protocol" proxyPort="0"
redirectPort="-1" scheme="https" secure="true" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_256_CBC_SHA" tcpNoDelay="true"
useURIValidationHack="true"/>
```

Once you have saved your changes, you must restart the application server.

E

Appendix E. MFT 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.

Pre-requisites

What you will need to configure the MFT Desktop Client:

1. .NET Client profile 4.0 or greater installed on any workstation that will use MFT Desktop Client v7.2.
2. Windows Software Developers Kit (SDK) with .NET Framework 3.5 or greater installed on a server that will be used to customize the Desktop Client for the environment. Note: The Windows SDK may come with a version of the .NET Framework greater than version 3.5. Due to Microsoft packaging issues however, .NET Framework 3.5 is required to configure and customize the MFT Desktop Client.

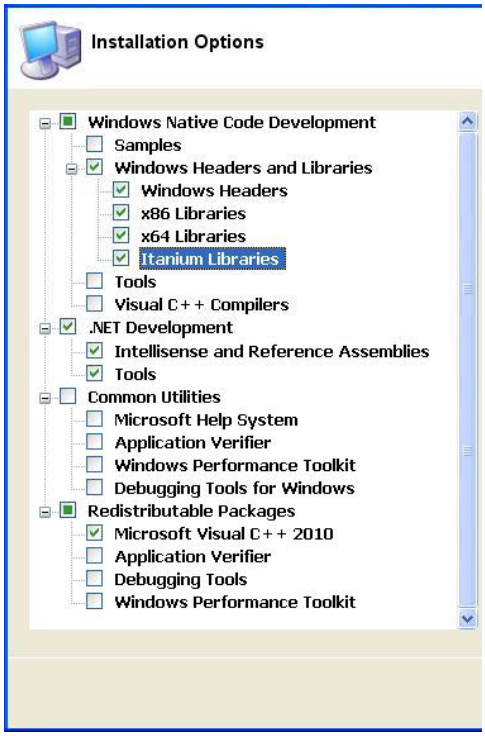
   For our examples we had .NET Framework 3.5 installed from a prior date and then installed Microsoft Windows SDK for Windows 7 and .NET Framework 4. Even though the name of this SDK says "Windows 7" this SDK is also supported on Operating Systems: Windows 7, Windows Server 2003 R2 Standard Edition (32-bit x86), Windows Server 2003 R2 Standard x64 Edition , Windows Server 2008, Windows Server 2008 R2, Windows Vista, Windows XP Service Pack 3. As of June 27, 2011 the URL to this download was:
   http://www.microsoft.com/download/en/details.aspx?id=8279.
3. MFT Internet Server v7.2 installed and operating.
4. Oracle Java SE 6 and above or IBM Java SE version 6 installed.
5. A code-signing certificate in .pfx format to sign the Desktop Client manifest files. *Note: A self-signed code signing certificate is provided for testing purposes or you can follow the provided instructions on how to generate a self-signed certificate yourself for testing purposes.*
6. The *bin* directory of the Windows SDK added to your PATH statement. *Note: If the bin directory is added to the PATH statement through the System Environment Variables panel you will need to reboot your server for the new setting to take place.*
7. The *bin* directory of the JDK added to your PATH statement. *Note: If the bin directory is added to the PATH statement through the System Environment Variables panel you will need to reboot your server for the new setting to take place.*

Note: Any end-users running Desktop Client v7.0 or below will need to uninstall the old version before they can install the new ClickOnce MFT Desktop Client v7.2 and above. When the end user removes the old version the configuration information will remain intact on their computers. If the default URL to connect to MFTIS is changing the end user will need the full URL in order to edit their old configuration. Please see the MFT Desktop Client User Guide for more information.

Windows SDK Installation

If you already have the Windows SDK installed on a system then skip this section and go on to the section, *Desktop Client Customization*. If you do not have a system with Windows SDK installed on it you must download and install the Windows SDK for a computer that will be used to setup the files needed for the MFT Desktop Client.

Note: It is not necessary to install the entire Windows SDK. During the install you will have the opportunity to select the items you want to install at the *Installation Options* window. See our example below of a Windows SDK v7.2 install with the minimum installation options selected that are needed:



Desktop Client Customization

In this section we will instruct you on how to customize the Desktop Client for your environment.

The Desktop Client needs to have a code-signing certificate in .pfx format available before you customize it. We have provided a self-signed code signing certificate named **test.pfx** with the password **test** assigned to it. If you will be using this provided certificate you can skip to **Step 2**.

Step 1) Before you can customize the Desktop Client you need to have a code-signing certificate in .pfx format. We have provided instructions below to allow you to generate a self-signed certificate for testing purposes. Self signed certificates are only practical for testing purposes while you wait for an external CA to sign a certificate for you.

To generate a self signed code-signing certificate you can use the **makecert.exe** program which is part of your Windows SDK program. The first command we will show you will generate your key pair, that is your private key and certificate:

makecert -sv yourprivatekeyfile.pvk -n "cert name" yourcertfile.cer -b mm/dd/yyyy -e mm/dd/yyyy –r

where:

- **-sv** *yourprivatekeyfile.pvk* is the name of the file containing the private key.
- **-n "***cert name***"** is the name that will appear on the certificate (and in the certificate store). *Note: The same IP or host name that was used for the cn when a certificate was generated for the MFTCC/IS installation should be used.*
- *yourcertfile.cer* is the name of the certificate file.
- **-b** *mm/dd/yyyy* is the date when the certificate becomes valid.
- **-e** *mm/dd/yyyy* is the date when the certificate expires.
- **-r** indicates that this will be a self-signed certificate.

When you have entered the command a window will open that will prompt you to enter the password to be used for the private key. *Note: You must set a password in order for the MFT Desktop Client customization to complete successfully. Do not select "None".* Once you have set the password and clicked the OK button. Then another window will open for you to enter that password in order to sign

the actual certificate file. Once you have clicked the Ok button you should see a message saying "Succeeded". See our example below:

Once this is complete you need to then create the .pfx file that will be used to sign your Desktop Client manifest files. For this you can use the **pvk2pfxt.exe** program which is part of your Windows SDK program. Below is the command you will need to run:

pvk2pfx –pvk yourprivatekeyfile.pvk –spc yourcertfile.cer –pfx yourpfxfile.pfx –po yourpfxpassword

where:

- **-pvk** *yourprivatekeyfile.pvk* is the private key file that you created in step 4.
- **-spc** *yourcertfile.cer* is the certificate file you created in step 4.
- **-pfx** *yourpfxfile.pfx* is the name of the .pfx file that will be created.
- **-po** *yourpfxpassword* is the password that you want to assign to the .pfx file. You will be prompted for this password when you add the .pfx file to a project in Visual Studio for the first time.

Example command below:

This completes the creation of the self signed code-signing certificate.

Step 2) Now copy the **MFTClickOnce.zip** file found in the <MFTIS_Install>\distribution\clickonce directory. Paste and extract this file in an empty directory on the Windows SDK server.

Step 3) Open a command prompt and add the *bin* directory from the Windows SDK as well as the *bin* directory to the JDK if this has not been set already. Navigate to the directory you extracted the **MFTClickOnce.zip** file and run the following script:

build.bat

Below is an example of the output that will be displayed from the build.bat script along with some additional information:

```
This script will prepare the ClickOnce files for installation.
This will be done in two steps. Step 1 will ask a series
of questions regarding how MFT Command Center or Internet Server
users will be connecting in order to perform transfers.
Step 2 will ask a series of similar questions regarding
the MFT Command Center or Internet Server that will be used to
distribute MFT Desktop Client.

The ClickOnce manifests must be signed with a code-signing
certificate in the pfx format. We have provided a self signed
code-signing certificate to test with [C:\DesktopClientSetup\153\test.pfx].
It is recommended that you obtain a code-signing certificate
from a certificate authority before using in production.

Do not use quotes around path or file names that contain space(s).

To accept default values presented press the ENTER key.

------------------------------------------------------------

Step 1: MFT Desktop Client File Transfer Server
```

```
Please enter the IP address or DNS name of the MFT Command Center or Internet
Server. [localhost] 10.1.2.84
Do you use the HTTP or HTTPS protocol to connect to the MFT Command Center or
Internet Server? [https]
Please enter the TCP port for . [8443]
Please enter the application context. [cfcc] mftis

Step 2: MFT Desktop Client Distribution Server

Please enter the IP address or DNS name of the MFT Command Center or Internet Server
which will store the ClickOnce files. [localhost] 10.1.2.167
Do you want to use the HTTP or HTTPS protocol when installing MFT Desktop Client?
[http]
Please enter the TCP port for https. [8080]
Please enter the application context. [cfcc] mftcc
Please enter the absolute path to your code-signing certificate.
[C:\DesktopClientSetup\153\test.pfx]
Please enter the password for your code-signing certificate. test
cfcc.exe.manifest successfully updated
cfcc.exe.manifest successfully signed
```

End users can be forced to upgrade to a new version of Desktop Client when one is available when they connect to the server. If you do not want to force them and allow them to choose whether to upgrade or not choose option 1 and the end user will be given a choice. The option will only be displayed once to upgrade.

```
Do you want to give end users the option to upgrade to this new version? (Choose No
to force the upgrade.)
1. Yes.
2. No.
Please enter your selection. [1]
cfcc.exe.manifest successfully updated
cfcc.exe.manifest successfully signed
```

You can store the clickonce application on either an HTTP Server such as the MFT Command Center, MFT Internet Server or an IIS server. It can also be stored on a Windows File Share. When you choose option 2 you will be prompted for the share file name (Note: The share must be pre-existing and if you are building the clickonce application on a server other than server that has the share defined on it you may need to map a drive to that share before it will be found).

```
Where will the application installation files be deployed?
1. HTTP Server.
2. Windows File Share.
Please enter your selection. [1]

cfcc-in.application successfully updated
cfcc-in.application successfully signed
cfcc-ca.application successfully updated
cfcc-ca.application successfully signed
...
...
...
Build completed successfully.

Now that your build is complete you must do the following:
1) Create a new directory under the MFT_HOME install directory of the
   MFT Command Center or Internet Server.
2) Copy the C:\DesktopClientSetup\153\clickonce.jar file to the new directory
   on MFT Command Center or Internet Server. Note: Your directory displayed may be different.
3) Unjar the clickonce.jar file using the following command from your command
   prompt window:
       jar xvf clickonce.jar
4) From the clickonce directory run either the install.bat script for Windows
   platforms or install.sh script for UNIX platforms to start the installation.
```

Follow all the instructions displayed on screen to complete building your customized MFT Desktop Client. *Note: If your MFTIS server is installed on a UNIX platform you must copy the clickonce.jar file to your system in binary format.*

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.

Note: To install the MFT Desktop Client application when using a Firefox browser you will need to install the ClickOnce Add-on. Go to ***https://addons.mozilla.org/en-US/firefox/tag/ClickOnce*** *and download and install the Add-on.*

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

Note: When using a self-signed certificate you will receive a Certificate Error when you connect to the server. You must install the certificate before you will be able to download and install the Desktop Client.

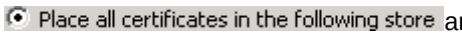
To install a certificate:

1) Click on the link 

When you arrive at the MFT Desktop Client install web page do not click on the install button before completing the steps below.
2) Click on the Certificate Error box at the top of your browser 

3) The "Untrusted Certificate" error window will be displayed. Click on the 

link at the bottom of the window.
4) The Certificate window will open. Click on the 

button.
5) On the Certificate Import Wizard window click **Next** button.
6) On the next window select 

and click the **Browse** button.
7) From the Select Certificate Store window highlight the "Trusted Root Certification Authorities" folder and then click the **OK** button.
8) On the Certificate Import Wizard screen click the **Next** button.
9) On the Certificate Import Wizard screen click the **Finish** button.
10) A Security Warning window should open. Click the **Yes** button to accept the certificate.
11) A Certificate Import Wizard window will open with a successful message. Click the **OK** button.
12) On the Certificate window click the **OK** button. The certificate is now installed.

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

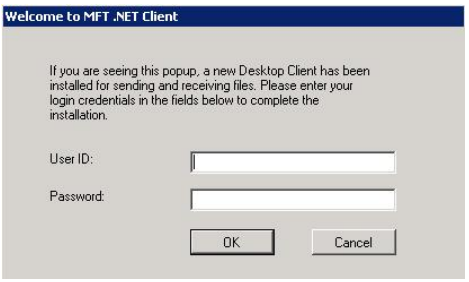
https://[DNS_HostName]:[httpsPort]/desktop-install

Note: If the default context was not used during installation, the redirector file for this shortcut as well as others mentioned later in this manual will need to be updated to redirect to the non standard context. Follow the instructions below to make these changes:
The redirection files can be found in the `<MFTIS_Install>`\server\webapps\ROOT directory. Use a text editor to open and change the "cfcc" context in these files to the new context chosen during the install. Once your changes have been made save and close the files.

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. You may or may not see an Application Install - Security Warning message. Click on the **Install** button. Then the TIBCO MFT Desktop Client License Agreement window will be displayed. 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.

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: If the default context was not used during installation, the redirector file for this shortcut as well as others mentioned later in this manual will need to be updated to redirect to the non standard context. Follow the instructions to make these changes:

The redirection files can be found in the <MFTIS_Install>\server\webapps\ROOT directory. Use a text editor to open and change the "cfcc" context in these files to the new context chosen during the install. Once your changes have been made save and close the files.

F

Appendix F. Thin Client Java JRE Required

MFT Internet Server provides a browser based transfer client called the Thin Client. To use the Thin Client Java JRE is required to be installed. This section will discuss setting the Java JRE requirement.

F.1 web.xml parameter MinimumJREVersion

The MFT Internet Server web application allows end users to perform file transfers through a browser based client called the Thin Client (for more information about the Thin Client please read the *MFT Command Center/Internet Server Thin Client User Guide*). The Thin Client requires a Java JRE to be installed on the end users' workstation before they will be able to perform any file transfers using the Thin Client. The default minimum JRE is version 1.6.0. If your environment requires a later version of a Java JRE to be installed, the web.xml parameter **MinimumJREVersion** may be updated.

Navigate to the following directory: <MFTIS_Install>/server/webapps/<CONTEXT_NAME>/WEB-INF/ and open the web.xml file to edit using an available text editor. Run a search for the parameter, MinimumJREVersion. You will see the following:

```
<context-param>
        <param-name>MinimumJREVersion</param-name>
        <param-value>1.6.0+</param-value>
</context-param>
```

Below are is an example of how you may edit the required JRE version for your environment:

```
<context-param>
        <param-name>MinimumJREVersion</param-name>
        <param-value>1.6.0_26+</param-value>
</context-param>
```

Note: If an end user is running Java JRE v1.6.0_18 or below and attempting to connect to MFT Internet Server using the Thin Client through Internet Explorer, the java script may not be able to detect the sub level version. The sub level is **18** in version JRE **v1.6.0_18**. As a result, the end user will not be forced to upgrade to a newer JRE version.

G

Appendix G. Configuring SSO

G.1 Web SSO

MFT Internet Server will work in a Web SSO environment. In Web SSO environments, there is typically a software component that performs all Authentications. Then the SSO software will forward all requests to the MFT software. The SSO Software will pass data in the HTTP Request or the HTTP Session to define the user that has been authenticated. MFT will extract and validate this information.

MFT Internet Server packages an XML file called **httpssocustomization.xml** that can be used to customize the MFT Internet Server authentication method for Web SSO. This file contains detailed information about how to configure the MFT server for Web SSO. It also defines the parameters that should be sent by the SSO Server and the validation that should be performed by MFT. This file is located in the following directory:

<MFTIS_Install>\server\webapps\<context>\WEB-INF directory.

Use a text editor such as Notepad to open the xml file to read instructions to configure the MFT Internet Server web application for your SSO environment.

H

Appendix H. Customized Translation Tables

H.1 ASCII/EBCDIC Translation Tables

MFT Internet Server is shipped with four ASCII to EBCDIC conversion tables to convert ASCII and EBCDIC characters and vice versa. By default the file named **Comtblg.dat** located at <MFTIS_Install>\server\webapps\<context>\translate directory is used by the system. Below is a list of the conversion tables and a brief description:

Comtblg.classic	The comtblg.dat shipped with prior versions. (Prior to v7.2)
Comtblg.cp037	Extended ASCII table that is based on IBM Code page 037
Comtblg.cp1047	Extended ASCII table that is based on IBM Code page 1047
Comtblg.dat	ASCII/EBCIDIC table used by MFTPS at run time (Default is copy of Comtblg.cp037)

Comtblg.dat is used by the system. If one of the other conversion tables needs to be used or a customized table has been created rename the existing **Comtblg.dat** and copy the new table to **Comtblg.dat**. The default file used for conversion must be named **Comtblg.dat**.

As mentioned above these tables can be customized. 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 MFT Internet Server install.

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 and name it **Comtblg.dat**. This file contains the table below which converts data between the ASCII and EBCDIC and EBCDIC to ASCII character sets:

```
000102033728D2E2F160500A0B0C0D0E0F
101112133C3D322618193F27221D351F
405A7F7B5B6C507D4D5D5C4E6B604B61
F0F1F2F3F4F5F6F7F8F97A5E4C7E6E6F
7CC1C2C3C4C5C6C7C8C9D1D2D3D4D5D6
D7D8D9E2E3E4E5E6E7E8E9BAE0BBB06D
798182838485868788899192939495 96
979899A2A3A4A5A6A7A8A9C04FD0A107
9F000000000000000000000000000000
000000000000000000000000000000000
41AA4AB100B26AB5BDB49A8A5FCAAFBC
908FEAFABEA0B6B39DDA9B8BB7B8B9AB
646562666367 9E687471727378757677
AC69EDEEEBEFECBF80FDFEFBFCADAE59
4445424643479C485451525358555657
8C49CDCECBCFCCE170DDDEDBDC8D8EDF
002E2E2E2E2E2E2E2E2E0A2E2E0D2E2E
2E2E2E2E2E0A2E2E2E2E2E2E2E2E2E2E
2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E
2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E2E
20A0E2E4E0E1E3E5E7F1A22E3C282B7C
26E9EAEBE8EDEEEFECDF21242A293BAC
2D2FC2C4C0C1C3C5C7D1A62C255F3E3F
F8C9CACBC8CDCECFCC603A23402273D22
D861626364656667686 9ABBBF0FDFEB1
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 Replace the existing Comtblg.dat

From the directory <MFTIS_Install>/server/webapps/<context>/translate rename the existing **Comtblg.dat** file to **org.Comtblg.dat**. Now copy and paste the new **Comtblg.dat** file that was customized in Step 1 into this folder. This file will now be your default conversion table used by the system.

Appendix I. Manual Install of MSSQL Driver

I.1 Microsoft SQL Driver sqljdbc4.jar

Step 1 Download the Microsoft JDBC Driver

This is the link to the download page for the driver:
http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=11774

Step 2 Stop the MFT Server

Step 3 Update the context .xml file

Navigate to <MFTIS_Install>/server/conf/Catalina/localhost/cfcc.xml
Note: The name of this file is the same as the context used. By default we use the context cfcc.

Open the file with Notepad and locate the **connectionURL** parameter and change the IP address, port number and database name as required:
Then search for the **driverName** parameter and replace the value with the following (be sure to keep the double quotes): "com.microsoft.sqlserver.jdbc.SQLServerDriver "

Step 4 Update the web.xml file

Navigate to <MFTIS_Install>/server/webapps/cfcc/WEB-INF/web.xml
Open the file using the Notepad program and replace the DBDriver and DBConn parameters as follows (for DBConn replace the IP address, port number and database name as required):

```
<context-param>
    <param-name>DBDriver</param-name>
    <param-value>com.microsoft.sqlserver.jdbc.SQLServerDriver </param-value>
</context-param>
<context-param>
    <param-name>DBConn</param-name>
    <param-value>jdbc:sqlserver://hostname:1433;databaseName=cfcc</param-value>
</context-param>
```

Step 5 Copy in new driver

Copy in the new sqljdbc4.jar driver to the following directory: <MFTIS_Install>/server/lib

Step 6 Start the MFT Server