TIBCO MFT Internet Server User 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 Internet Server, 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

1 Administrator Browser Configuration

This section describes how to use the Administrator Web Pages to configure MFT Internet Server for use.

1.1 Accessing MFT Internet Server Administrator Browser

Once MFT is installed and configured, it is time to access the MFT Internet Server Administrator web pages. To login use the following URL substituting the areas of the URL with your install configurations:

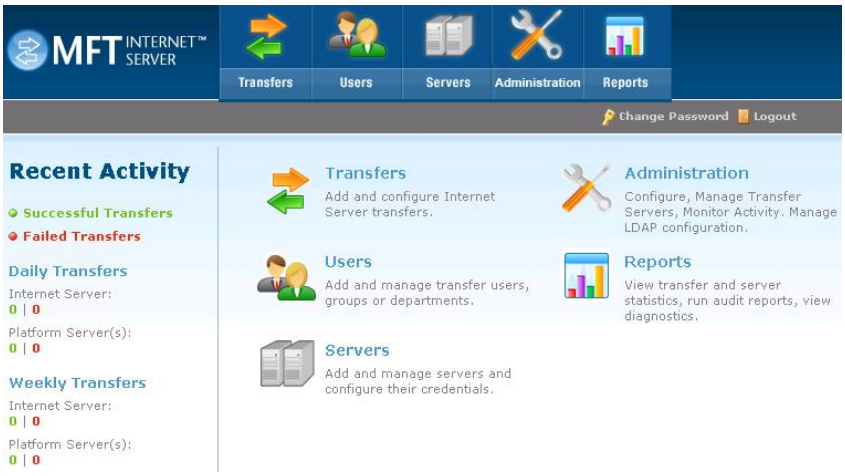
https://[DNS_HostName]:[httpsPort]/cfcc/control?view=view/admin/start.jsp

Application Server	Default Port
Embedded Server	443

When you are prompted for a userid/password use the Administrator defaults: **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.

The MFT Internet Server main web page is similar to the following:



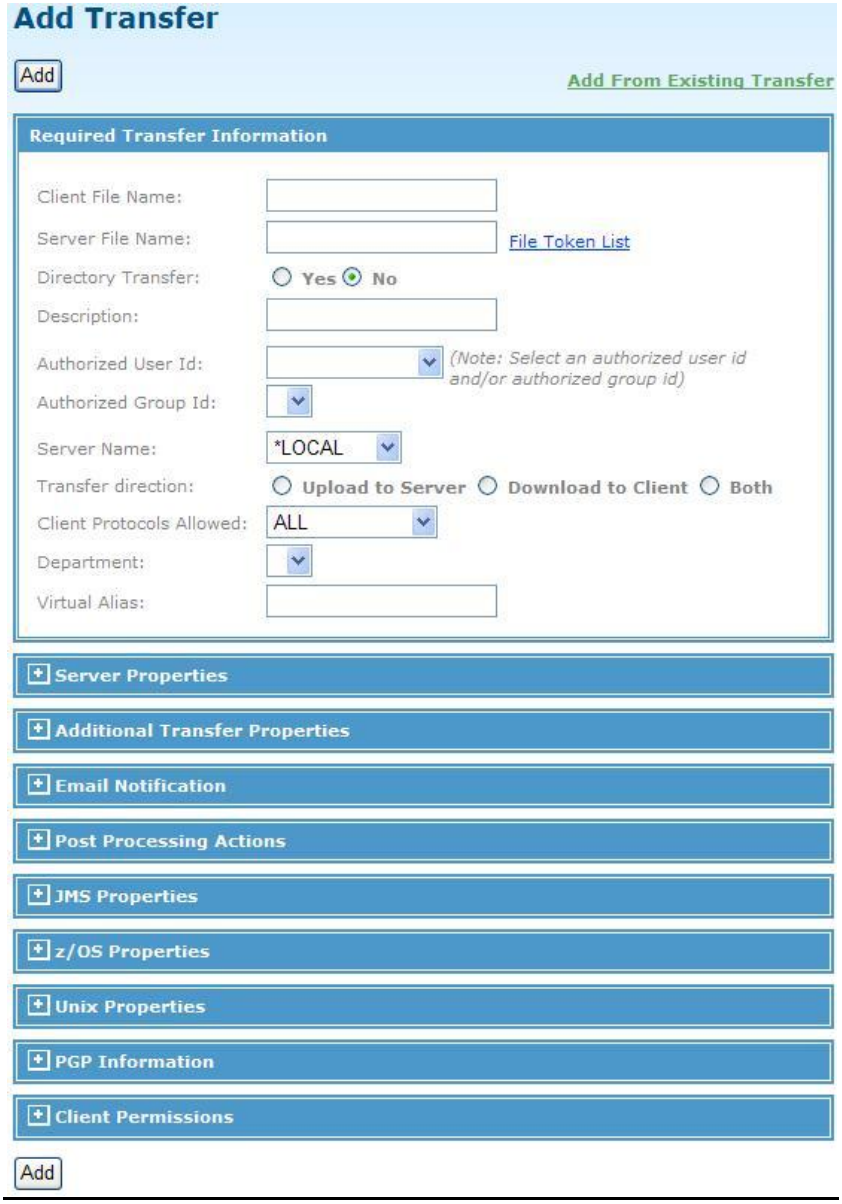
1.2 Transfers

The Transfers web page is where all transfer definitions are defined to the MFT Internet Server.

1.2.1 Add Transfer

When a transfer user signs on to the MFT Internet Server using various clients, the transfers that will be displayed will depend on what was defined under Add Transfers. This section will allow the administrator to add and manage transfer definitions. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation: Transfers > Add Transfer

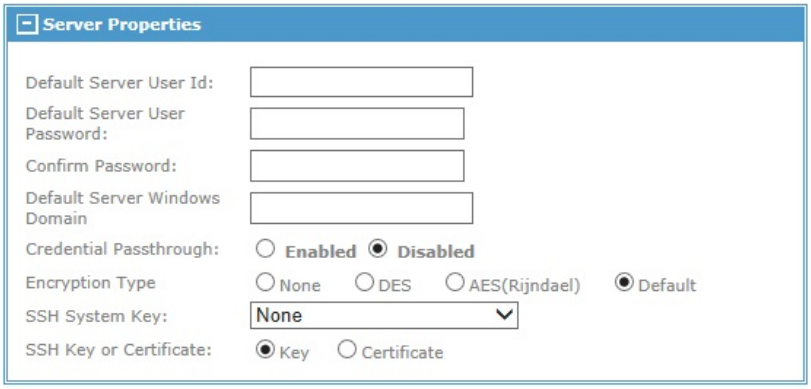


This page enables the administrative user to add transfers to the system. The administrative user must have the **AdministratorRight** or **UpdateTransferDefinitionRight** in order to add an internet transfer definition.

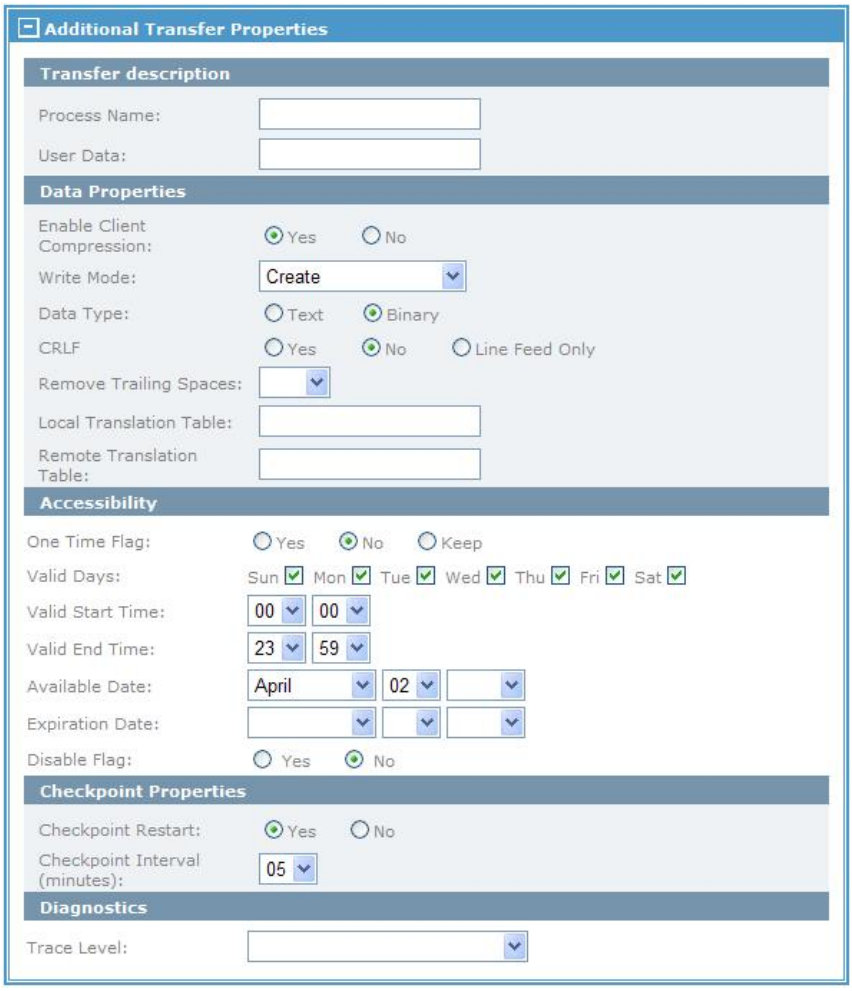
There are ten sections on the Add Transfer page:

Required Transfer Information Defines the most important parameters needed to create an transfer record.

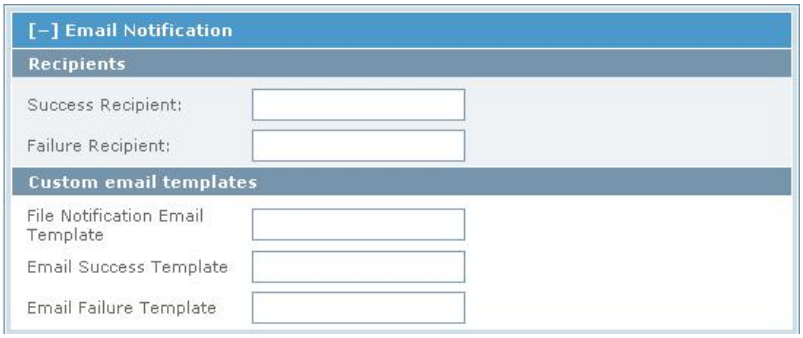
Server Properties Defines parameters specific to the Server Name selected in the Required Information section.



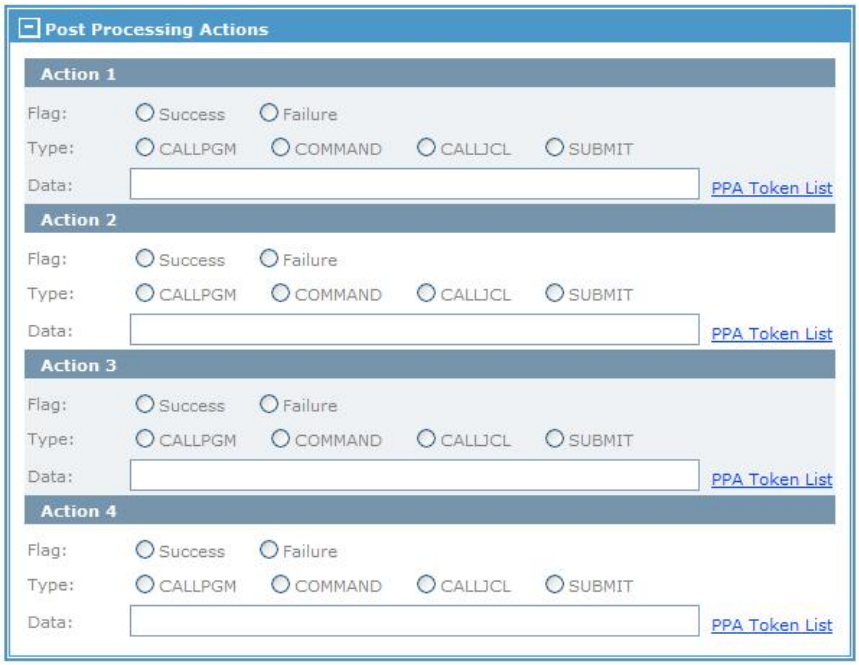
Additional Transfer Properties This box is broken up into sub-boxes Transfer description, Data Properties, Accessibility, Checkpoint Properties and Diagnostics. Note: Checkpoint Restart is not supported when using PGP encryption or transfer to/from an AS2 server and should be set to No.



Email Notification Allows MFT Internet Server to send email notification to one or more users.



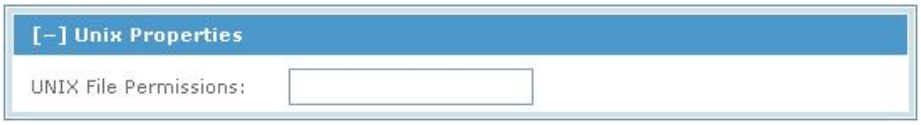
Post Processing Actions Allows you to perform up to four actions to be completed by the Server when a file transfer request has completed.



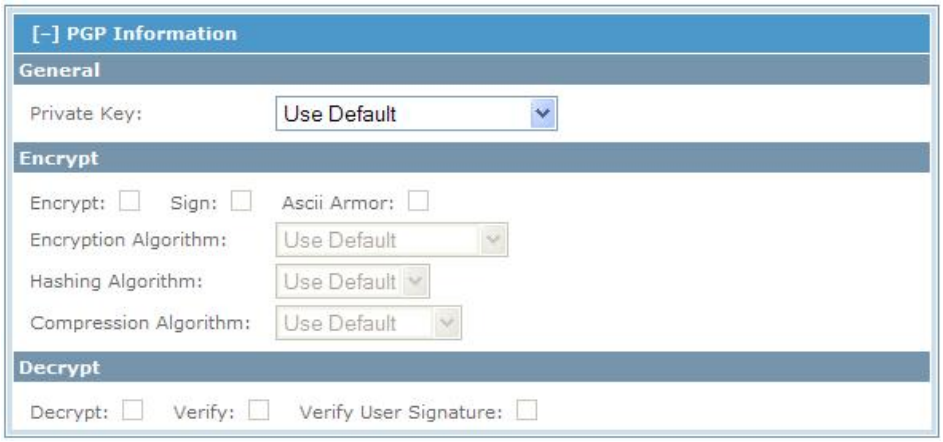
JMS Properties Used for file transfer conducted between a JMS server and MFTIS.

z/OS Properties Used only when creating a file on the z/OS system through an Upload operation. You use these parameters to define information about the file to be created.

Unix Properties Used only when creating a file on a Unix system through an Upload operation.



PGP Information Defines the PGP Information that can be associated with a Transfer.



Client Permissions Defines the permissions that are allowed when conducting this transfer using an FTP, SSH or Desktop Client.

Note: Allow Client Transfer Mode can be used for FTP file transfers to other FTP server or the MFT FTP server (*LOCAL).

When setting the Allow Delete or Allow Rename the Server Platform must be be defined to the correct Operating System in the Server Definition for proper functionality.

1.2.1.1 Add From Existing Transfer

Navigation: Transfers > Add Transfer

This link allows the administrative user to copy a Transfer definition to create a new one without having to enter all the Transfer information again. Click on the "**Add From Existing Transfer**" link and a listing of existing Transfers will be displayed. Click on the File Id to copy the definition. The new definitions will not contain the Authorized User Id or Authorized Group Id. For a Transfer that also uses Server Properties, the Server User Id and Server User Password will also be blank. User Id and Password type information will have to be entered for each new Transfer defined.

1.2.2 Manage Transfers

The user must have AdministratorRight or UpdateTransferDefinitionRight in order to manage Internet Transfer definitions. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation: Transfers > Manage Transfer

This will take you to a page containing a section for Selection Criteria and a list of the first 100 defined Transfers. If there are more than 100 Transfers defined, click on "**List Next 100 >**" to access the next 100 Transfer definitions. Use the Back button to see the previous definitions.

A listing of particular Transfers can be obtained by either choosing the link "**List Transfers by Users**" or entering the search criteria for any combination of the following: File Id, Server File Name, Description, Authorized User Id, Authorized Group Id, Server Name and Department. A percent sign (%) may be used as a wildcard character.

Selecting the "**List Transfer by Users**" link will give you a list of users. Click on the User Id link for a listing of Transfer definitions for that particular user.

From the Manage Transfers panel, Transfer definitions can also be updated or deleted. To update a definition, click on the File Id of the Transfer definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

To delete a Transfer definition, select the check box next to the Transfer that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Transfer definitions may be deleted at one time.

If you want to refresh the Manage Transfers list, you can use the Navigation box on the left portion of the screen and click on Manage Transfers.

1.2.3 OnDemand

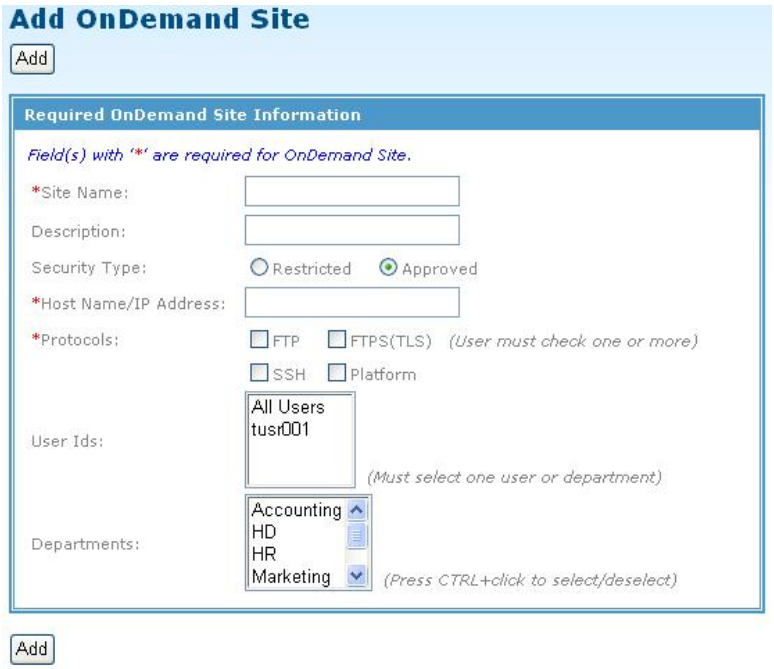
When you want to allow end users that are using the MFT Desktop Client (must be version 7.1 or higher) to directly connect to a remote FTP, SSH, or Platform Server you would configure those servers details here. The users or departments you authorize to connect to these servers will have an added menu item displayed in their MFT Desktop Client File menu called Site Manager. *Please see the MFT Desktop Client User Guide for more information about Site Manager.*

Only users with the **AdministratorRight** or **UpdateOnDemandRight** can add or manage the OnDemand Sites to MFTIS.

Note: This is a licensed feature. You must be licensed to be able to use OnDemand Sites.

1.2.3.1 Add OnDemand Site

Navigation: Transfers > OnDemand > Add OnDemand Site



By default there are no users defined to the OnDemand Site settings. Users must be granted the **OnDemandTransferRight** before they will appear in the User Ids lists.

*Note: By highlighting **All Users** will allow all users with the OnDemandTransferRight to connect to this server.*

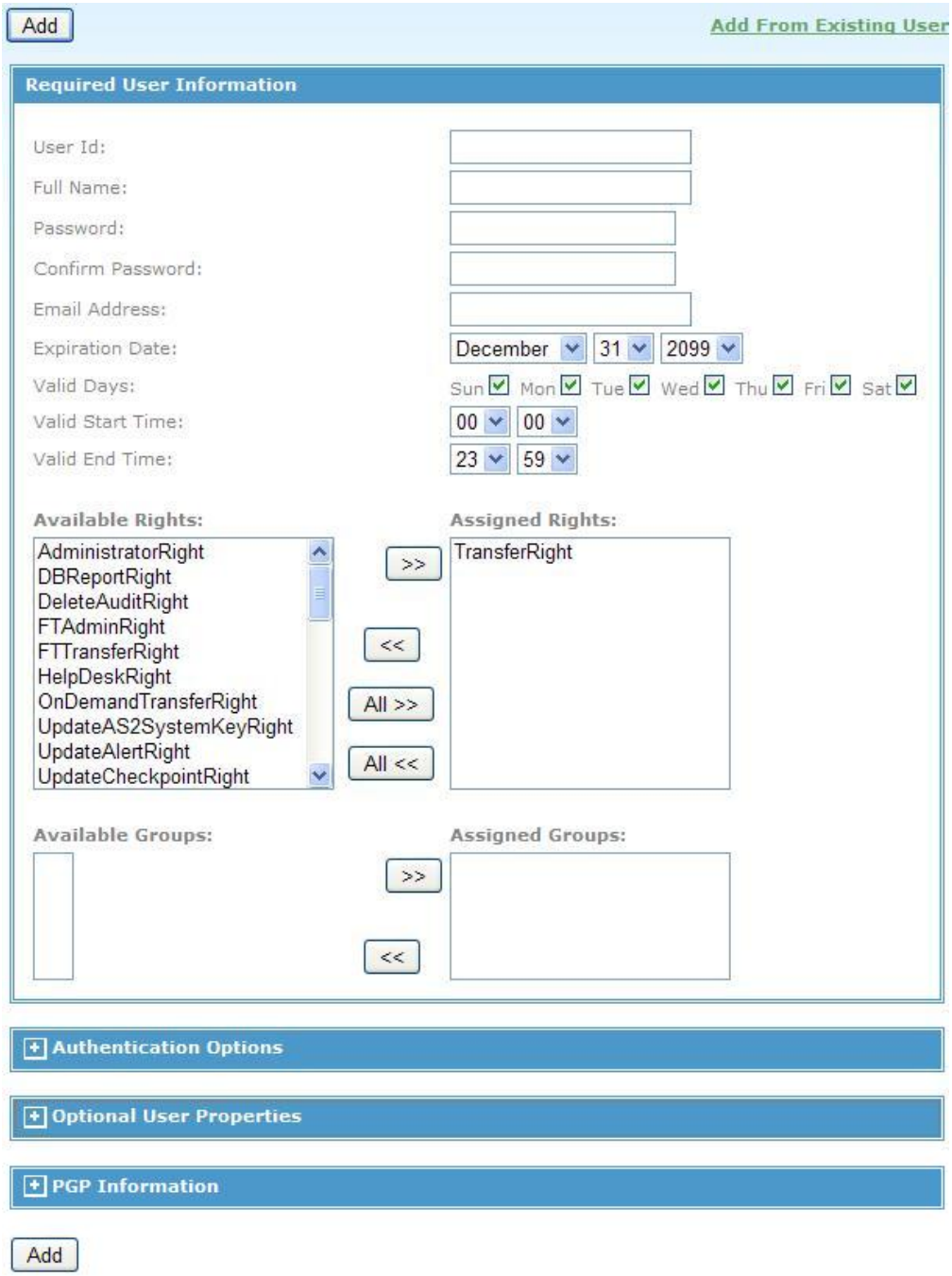
Please see the online help for a detailed description about each field.

1.3 Users

The Users section defines and manages Users, Transfer Groups and Departments. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

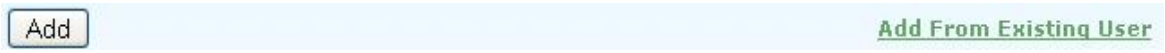
1.3.1 Add User

Navigation: Users > Add User



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

At the top of the web page you will see the link **Add From Existing User**



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

Template User ID	**Rights Assigned**
ArchiveUser	(No Rights Assigned)
AuditorUser	ViewAlertRight ViewAuditRight ViewGroupRight ViewServerCredentialRight ViewServerRight ViewTransferDefinitionRight ViewUserRight
Collector	(No Rights Assigned)
HelpDeskUser	HelpDeskRight UpdateSessionRight ViewAlertRight ViewAuditRight ViewUserRight
TransferUser	TransferRight
admin	AdministratorRight TransferRight

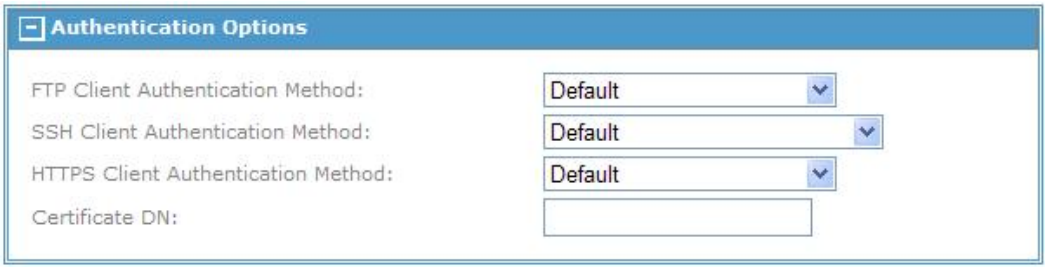
A Collector and ArchiveUser Id’s are also added by default. These ids are used to create Server Credentials for a Server(s) that will also have the collection and archive option turned on. There are no rights given to these ids.

If you do not wish to use any of the Template User definitions available to you a new user definition can be created manually. The **Add User** page is divided into the following two sections:

Required User Information Defines the fields that are required to create a User record.

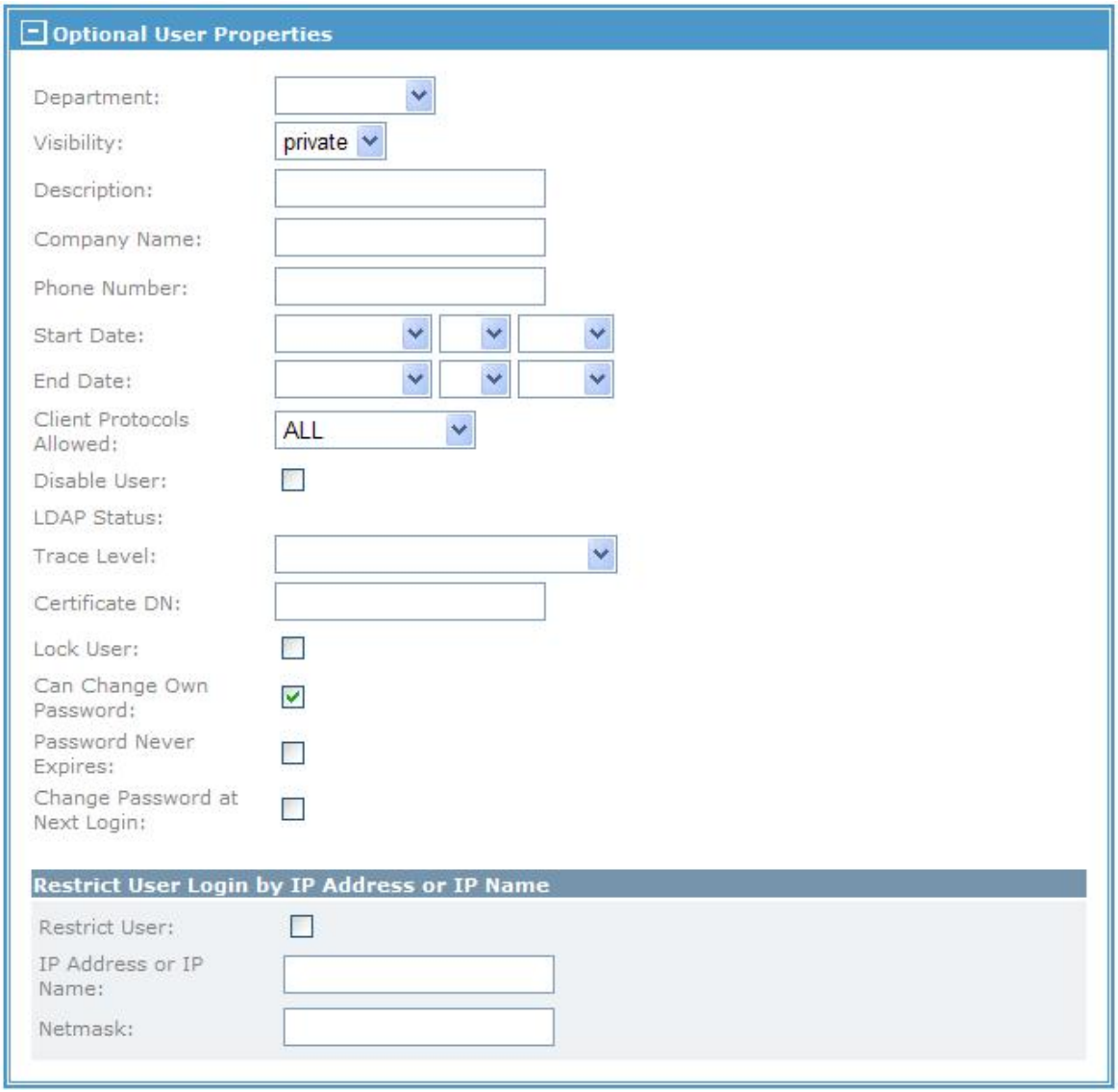
Authentication Options

Defines a users client authentication method for FTP, SSH, and HTTPS client connections. These settings will override the global settings found in the System Configurations. Use the Certificate DN when Trusted Certificates are being added in the Administration > Keys > Trusted Certificates > Add Trusted Certificates web page.



Optional User Properties

Defines a variety of parameters that are not required.



PGP Information Defines the PGP settings that can be configured for the user.

By default the user is set to **Default** and uses the System Configurations. To read more about System Configurations please see section *System Configuration*. By setting **Allow User to Add PGP Key** to Yes you are allowing the user to add PGP Public keys to the MFT database.

1.3.2 Available Rights

There are 24 rights that can be assigned to a MFT Internet Server user. Below is the list of rights along with a description of what each right is for and how it will work when using and not using Delegated Administration (Departments).

Right	Description	Description using Delegated Administration
AdministratorRight	Allows a user to perform all administrative functions within the MFTIS system. This right does not include TransferRight or FTTransferRight or any functions that correspond to these rights.	Allows a user to perform all administrative functions within their Department. This right does not include TransferRight or FTTransferRight or any functions that correspond to these rights. The Department Administrator cannot update Server or Server Credentials unless given UpdateServerRight and UpdateServerCredentialRight.
DBReportRight	Allows a user to login and view and generate MFTCC's Database Reports from Reports>Database Reports menu	Allows a user to login and view and generate MFTCC's Database Reports from Reports>Database Reports menu
DeleteAuditRight	Allows any user to delete Audit Record.	Allows any user to delete Audit Record. Department checking will not be done.
FTAdminRight	Allows a user to view and update menu items from the Management>Platform Transfers however, this right will NOT allow a user to execute Platform Transfers. If this right is assigned along with the ViewServerRight the user can also view and update all the items in the Manage Platform Functions menu.	Allows a user to view and update menu items from the Management>Platform Transfers however, this right will NOT allow a user to execute Platform Transfers. If this right is assigned along with the ViewServerRight the user can also view and update all the items in the Manage Platform Functions menu.
FTTransferRight	Allows a user to view and execute the Management>Platform Transfers. However, this right will NOT allow a user to update a Platform Transfer.	Allows a user to view and execute the Management>Platform Transfers. However, this right will NOT allow a user to update a Platform Transfer.
HelpDeskRight	Allows a user to change another user's password, turn on and off the disable flag for a user as well as turn on and off the lock flag for a user.	Allows a user to change another user's password, turn on and off the disable flag for a user as well as turn on and off the lock flag for a user.
OnDemandTransferRight	Allows a user the ability to use the Desktop Client Site Manager to setup and conduct on demand transfers.	Allows a user the ability to use the Desktop Client Site Manager to setup and conduct on demand transfers.
TransferRight	Allows a user to execute MFT Internet Transfers.	Allows a user to execute MFT Internet Transfers.
UpdateAlertRight	Allows a user to Update Alert records and view Alerts that have occurred.	Allows a user to Update Alert records and view Alerts that have occurred.

Right	Description	Description using Delegated Administration
UpdateAS2SystemKeyRight	Allows a user to add and manage the configurations of MFT AS2 System Keys.	Allows a user to add and manage the configurations of MFT AS2 System Keys.
UpdateCheckpointRight	Allows a user to access the MFT Internet Checkpoints web page and delete Checkpoints taken.	Allows a user to access the MFT Internet Checkpoints web page and delete Checkpoints taken for their department.
UpdateFTTransferRight	Allows a user to update Platform Transfers defined under Management>Platform Transfers>Manage Platform Transfers This right will NOT allow the user to execute Platform Transfers.	Allows a user to update Platform Transfers defined under Management>Platform Transfers>Manage Platform Transfers This right will NOT allow the user to execute Platform Transfers.
UpdateGroupRight	Allows a user to view and update MFT Group records.	Allows a user to view and update MFT Group records. Note:
UpdateOnDemandRight	Allows a user the ability to add or remove the OnDemand Sites.	Allows a user the ability to add or remove the OnDemand Sites assigned to other users within their department.
UpdatePGPKeyRight	Allows a user to add and manage the configurations PGP Public Keys.	Allows a user to add and manage the configurations PGP Public Keys.
UpdatePGPSystemKeyRight	Allows a user to add and manage the configurations of MFT PGP System Keys.	Allows a user to add and manage the configurations of MFT PGP System Keys.
UpdatePublicKeyRight	Allows a user to add and manage the configurations of MFT FTP, SSH, HTTPS Public Keys.	Allows a user to add and manage the configurations of MFT FTP, SSH, HTTPS Public Keys.
UpdateServerCredentialRight	Allows a user to view or MFT Server Credential records.	Allows a user to view or update MFT Server Credential records.
UpdateServerRight	Allows a user to view or update MFT Server records.	Allows a user to view or update MFT Server records in their own Department. New Servers cannot be added.
UpdateSessionRight	Allows a user to view and delete active user sessions.	Allows a user to view and delete active user sessions.
UpdateSystemKeyRight	Allows a user to add and manage the configurations of MFT FTP and SSH **System Keys** contained under the Management>Keys> menu.	Allows a user to add and manage the configurations of MFT FTP and SSH **System Keys** contained under the Management>Keys> menu.
UpdateTransferDefinitionRight	Allows a user to view and update MFT Internet Transfer definitions.	Allows a user to view and update MFT Internet Transfer definitions.
UpdateTransferUserRight	Allows a user to view and update MFT User records. Only TransferRight and OnDemandTransferRight can be given to a user unless you are an administrator. The Super Administrator can assign any right to a user. Note: When assigning this right to a user you must also assign either the ViewGroupRight or the UpdateGroupRight.	Allows a user to view and update MFT User records. Only the TransferRight and OnDemandTransferRight can be given to a user unless you are an administrator. The Department Administrator can assign any rights to a user within their Department except UpdateServerRight and UpdateServerCredentialRight. Note: When assigning this right to a user you must also assign either the ViewGroupRight or the UpdateGroupRight.
ViewAlertRight	Allows a user to view Alert records and view Alerts that have occurred.	Allows a user to view Alert records and view Alerts that have occurred.
ViewAuditRight	Allows a user to view Audit records and update the Audit Search Filter.	Allows a user to view Audit records and update the Audit Search Filter.
ViewCheckpointRight	Allows a user to access the MFTI Internet Checkpoints web page and view Checkpoints taken.	Allows a user to access the MFT Internet Checkpoints web page and view Checkpoints taken for their department.

Right	Description	Description using Delegated Administration
ViewFTTransferRight	Allows a user to view Platform Transfers defined under Management>Platform Transfers>Manage Platform Transfers This right will NOT allow the user to add, update, or execute Platform Transfers.	Allows a user to view Platform Transfers defined under Management>Platform Transfers>Manage Platform Transfers within their Department. This right will NOT allow the user to add, update, or execute Platform Transfers.
ViewGroupRight	Allows a user to view MFT Group records.	Allows a user to view MFT Group records.
ViewOnDemandRight	Allows a user to view MFT OnDemand Site records.	Allows a user to view MFT OnDemand Site records.
ViewPGPKeyRight	Allows a user to view PGP Public Keys.	Allows a user to view PGP Public Keys.
ViewPublicKeyRight	Allows a user to view MFT FTP, SSH, HTTPS Public Keys.	Allows a user to view MFT FTP, SSH, HTTPS Public Keys.
ViewServerCredentialRight	Allows a user to view MFT Server Profile records.	Allows a user to view MFTIS Server Profile records.
ViewServerRight	Allows a user to view MFT Server records.	Allows a user to view MFT Server records.
ViewSessionRight	Allows a user to view active user sessions.	Allows a user to view active user sessions.
ViewTransferDefinitionRight	Allows a user to view MFT Internet Transfer records.	Allows a user to view MFT Internet Transfer records.
ViewUserRight	Allows a user to view MFT User records and the Rights associated with those users.	Allows a user to view MFT User records and the Rights associated with those users.

1.3.3 Manage Users

Under the Manage Users section, users can be listed, searched, updated and deleted. The user must have AdministratorRight or UpdateTransferUserRight in order to manage User definitions. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation:

Users > Manage Users

The above screen shot shows the Manage Users web page with the 6 “Template Users” that are automatically added to the database during the MFT Internet Server installation process. This page can contain a list of the first 100 defined Users. If there are more than 100 Users defined, click on “List Next 100 >” to access the next 100 User definitions. Use the Back button to see the previous definitions.

A list of particular Users can be obtained by entering the search criteria for any combination of the following: User Id, Full Name, Role, Group and Department. A percent sign (%) may be used as a wildcard character.

To update a user definition, click on the User Id of the User definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

To delete a User definition, select the check box next to the User that you wish to delete and click on the Delete button at the bottom of the panel. Multiple User definitions may be deleted at one time.

To refresh the Manage Users list, you can use the Navigation box on the left portion of the screen.

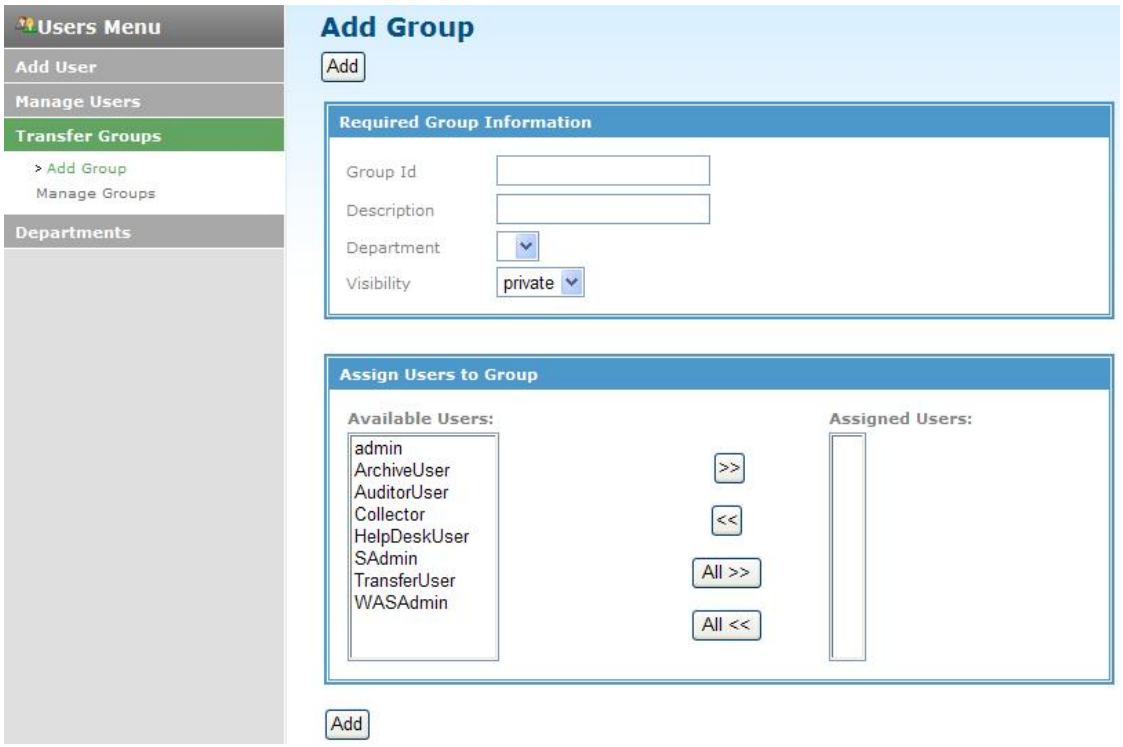
1.3.4 Transfer Groups

To display the Transfer Group information page, click on Users and Transfer Groups. The following panel will be displayed. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.3.4.1 Add Group

Navigation:

Users > Transfer Groups > Add Group



This page enables the administrative user to add new Groups to the system. The administrative user must have the AdministratorRight or UpdateGroupRight in order to add a Group.

There are two sections on the Add Groups page:

Required Group Information Defines fields that must be entered to create a Group.

Assign Users to Group Defines which users will be in the defined Group.

1.3.4.2 Manage Groups

Navigation:

Users > Transfer Groups > Manage Groups

Above is an example of 3 groups that had been created and can be managed from the Manage Groups page. The page will contain a list of the first 100 defined Groups. If there are more than 100 Groups defined, click on “List Next 100 >” to access the next 100 Group definitions. Use the Back button to see the previous definitions.

From the Manage Groups panel, Group definitions can be updated or deleted. To update a definition, click on the Group Id of the Group definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

To delete a Group definition, select the check box next to the Group that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Group definitions may be deleted at one time.

If you want to refresh the Manage Groups list, you can use the Navigation box on the left portion of the screen.

The administrative user must have AdministratorRight or UpdateGroupRight in order to manage Group definitions.

1.3.5 Departments

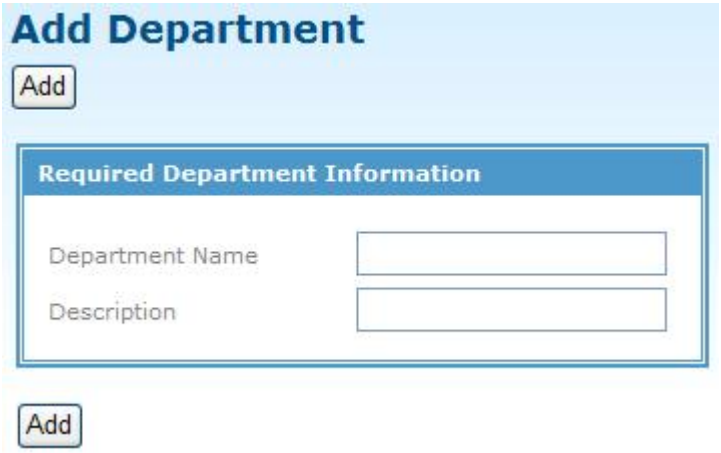
To display the Department information page, click on Users and Departments. The following panel will be displayed. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

For more information as to how departments should be utilized, please refer to the chapter on Delegated Administration.

1.3.5.1 Add Department

Navigation:

Users > Departments > Add Department



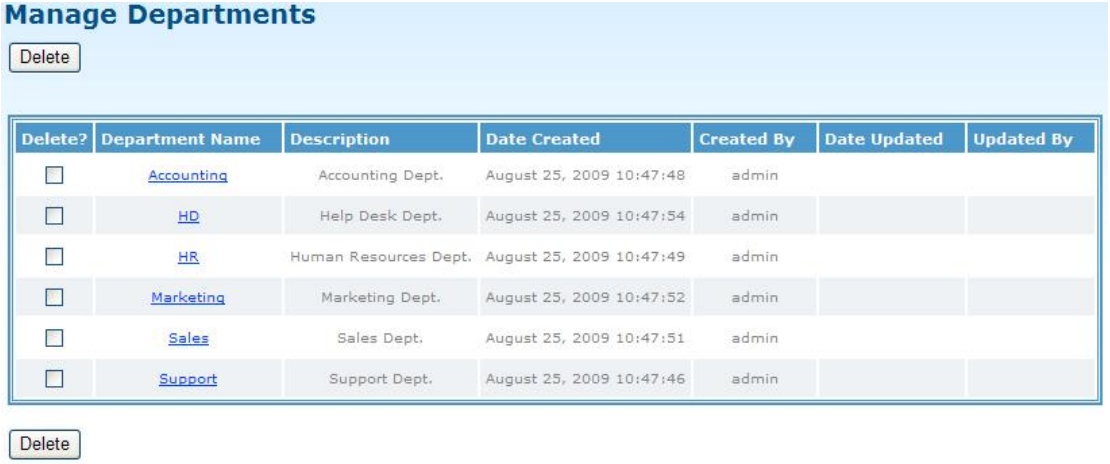
Departments can only be added by an administrator who has access to the entire MFT Internet Server system. This administrator has no department and is known as a “Super Administrator”. This page enables the Super Administrator to add new departments to the system. This feature is used for Delegated Administration.

The only section on the page is the **Required Department Information** which defines fields that must be entered to create a Department.

1.3.5.2 Manage Departments

Navigation:

Users > Departments > Manage Departments



Above is an example of 3 departments that have been created and can be managed from the Manage Departments page. The page will contain a list of the first 100 defined Departments. If there are more than 100 Departments defined, click on “List Next 100 >” to access the next 100 Department definitions. Use the Back button to see the previous definitions.

From the Manage Departments panel, Department definitions can be updated or deleted. To update a definition, click on the Department Name of the Department definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

To delete a Department definition, select the check box next to the Department that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Department definitions may be deleted at one time.

If you want to refresh the Manage Departments list, you can use the Navigation box on the left portion of the screen.

The administrative user must have AdministratorRight in order to manage Department definitions.

1.4 Servers

Server Definitions contain the information that MFT Internet Server needs to communicate with the following server types:

The Server definition defines how the supported client's can gain access to a file. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.4.1 Add Server

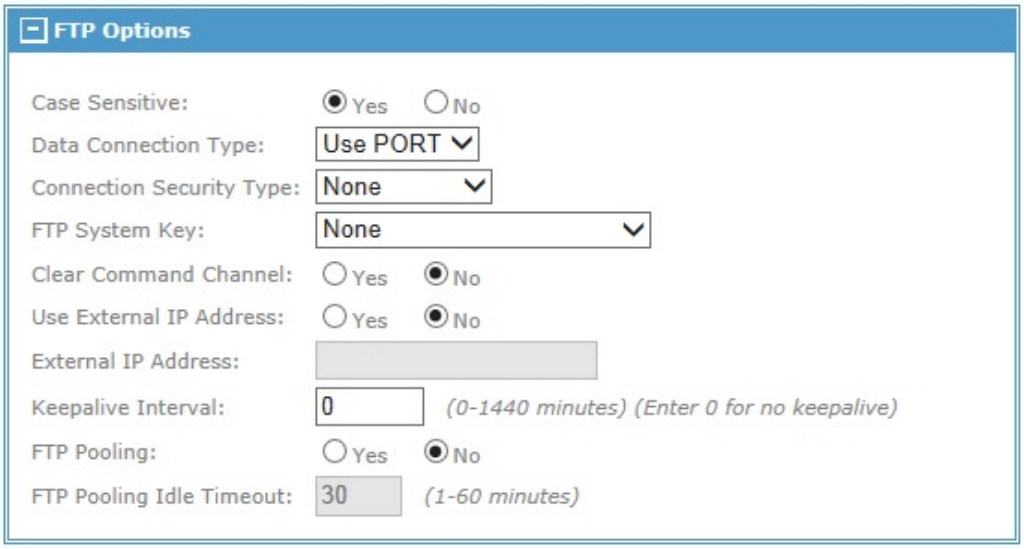
This page enables an administrative user to add remote Servers to the MFT Platform Server system. The administrative user must have the AdministratorRight or UpdateServerRight in order to add a Server.

Navigation: Servers > Add Server

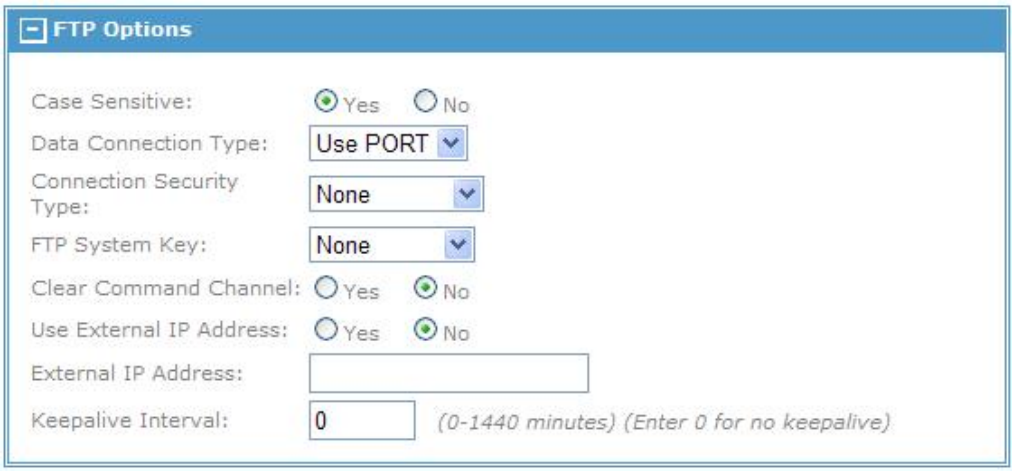
The Add Server page is divided into the following eleven sections:

Required Server Information Defines the required parameters needed to create a Server record.

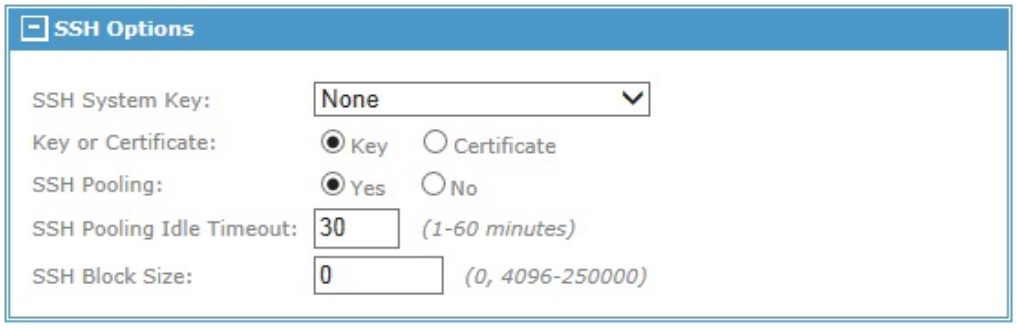
Platform Server Options Defines Server options that are used only when the Server Type is defined as Platform Server.



FTP Options Defines Server options that are used only when the Server Type is defined as FTP. Note: At this time IBM i Series FTP Servers are not supported.



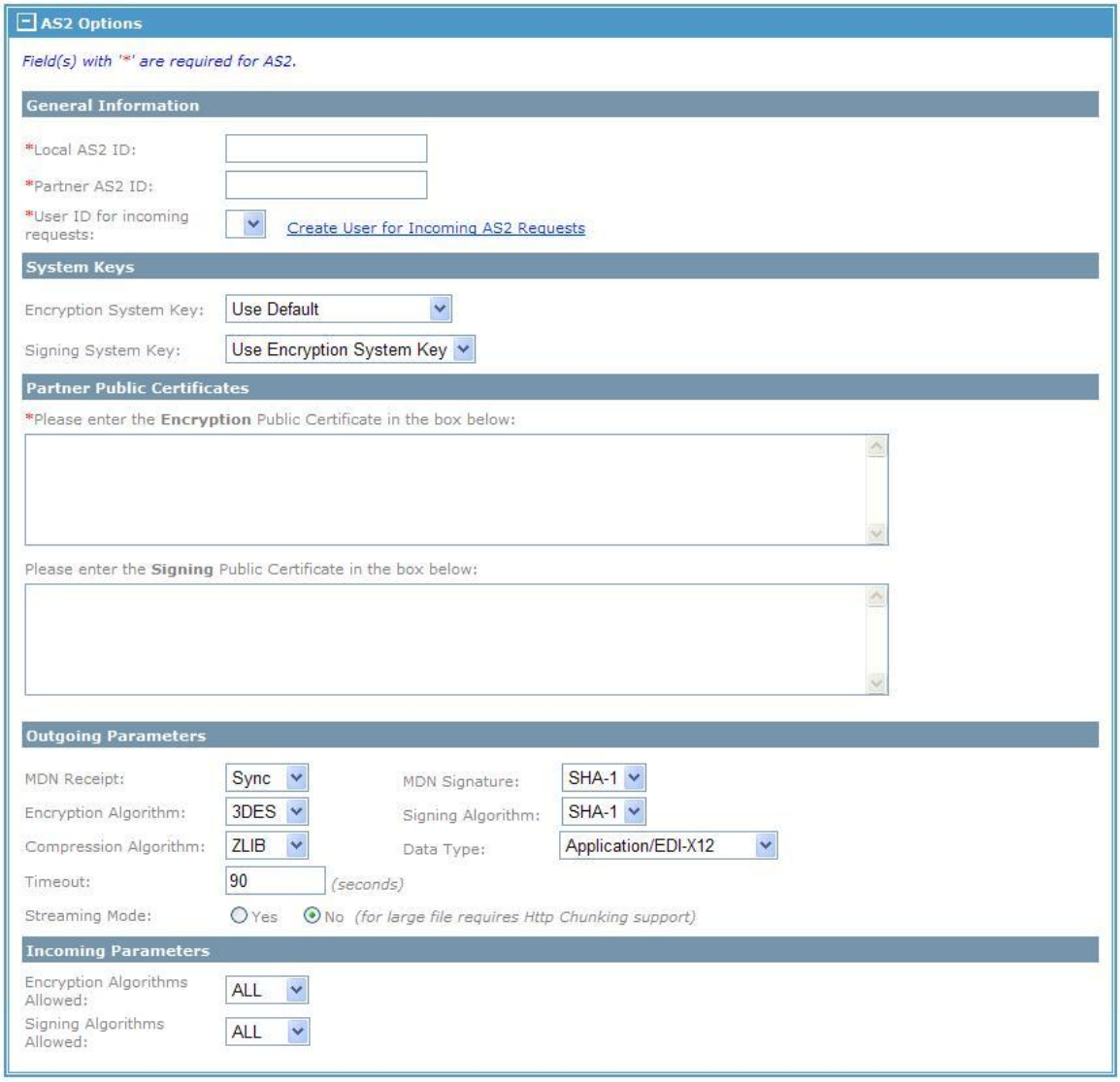
SSH Options Defines the SSH System Key to be used with this server and if zlib compression should be used when transferring data to this SSH server.



AS2 Options Defines Server options that are used only when the Server Type is defined as AS2.

Note:

- Local AS2 ID should be set to the same Local AS2 ID defined in the MFTIS Configure AS2 Server web page settings.
- When using Streaming Mode to send files to remote AS2 servers they must be configured for HTTP Chunking Support. If the remote AS2 server is another MFTIS server no configuration changes are needed as MFTIS is configured for HTTP chunking.
- Checkpoint Restart is not supported for transfer to/from an AS2 server and should not be enabled in a transfer definition defined for an AS2 Server.



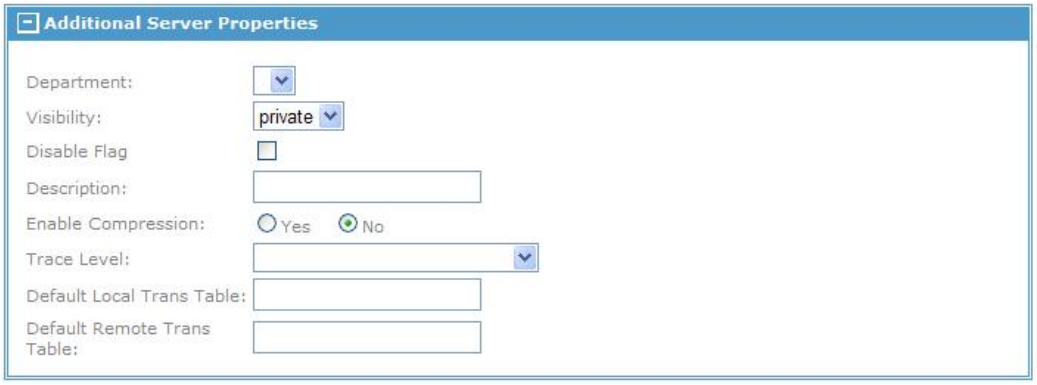
Internet Server Options When a Server being defined as a Server Type of Internet Server the Internet Server context would be defined in this section. You must indicate if the port being defined for the Internet Server is a Secure port or not.

Server Options This window is used to predefine a default path that file uploads and downloads would use. This can be very helpful when defining transfer definitions. For example the path could be defined here and in the transfer definition the Administrator could define file name tokens without defining a path in the Server File Name field.

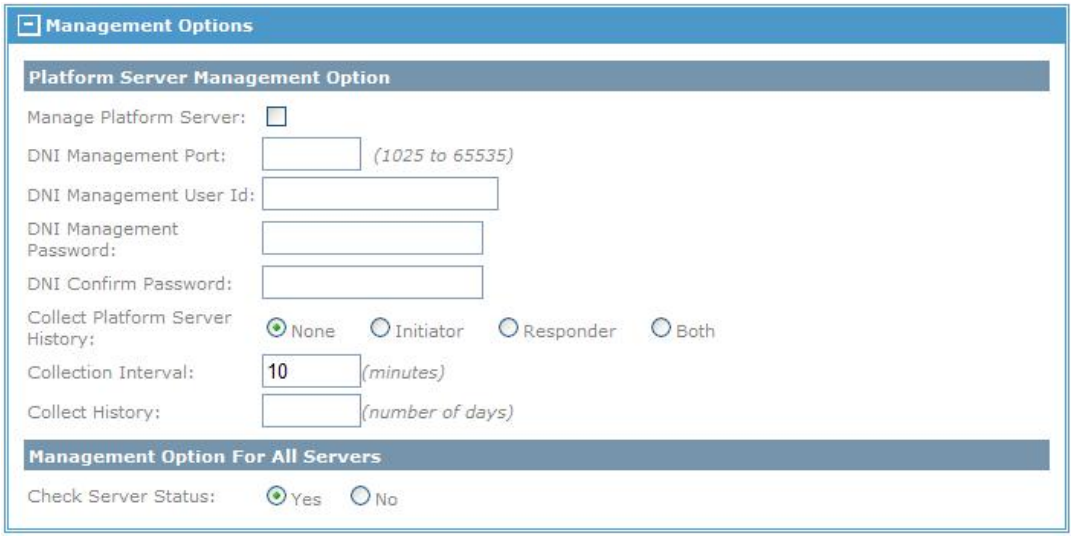
Note: This field cannot be overridden.

Server Credentials Defines a default User Id and Password to be used for this server. These credentials are used for transfers as well as Platform Server audit collection purposes (See the Collection Service section of this manual for more information about collecting Platform Server audits.) Note: These credentials can be overridden for transfers from a transfer definition or a Platform Server transfer definition.

Additional Server Properties Defines parameters specific for this server, such as department, description and trace level. See the online help for more information on the fields in this section.

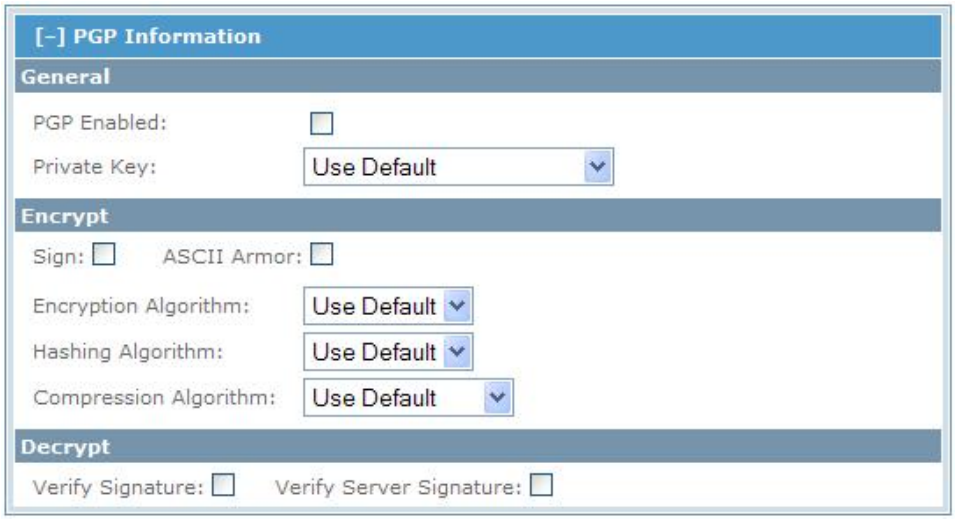


Management Options This window contains two sections. The Check Server Status allows MFTCC and MFTIS to monitor if there is a good connection using the port defined for the server being added to the system (Status Service must be configured to use this service.) The other section is used if the Server Type is Platform Server. When you want to collect Platform Server audit records the Manage Platform Server box must be enabled. Then set the Collect Platform Server History, Collection Interval, and the Collect History fields. You will be told you need to restart the Collection Service if you have it running already. To read more about collecting audit logs from a Platform Server please read the Collection Service section of this manual. If the Administrator will be managing DNI (Directory Named Initiation) from MFTCC the DNI port, DNI user id, and password must be defined. MFTCC and MFTIS both distribute the DNI perl programs, templates and instruction manual within the dni.tar file located in the following installation directory: `<MFT_Install>\distribution\dni`. To extract the files from the dni.tar use the following command from your command prompt: **tar –xvf dni.tar**



PGP Information

If the server being defined will be used to conduct file transfers with PGP encrypted files you would define the PGP keys that will be used to encrypt (file Uploads) or decrypt (file Downloads) files. The PGP Keys can either be generated by MFTIS or imported into the system by the Administrator through the MFTIS Administrator web pages or by an end user through the Thin Client. To read more about the Thin Client see the MFT Internet Server Thin Client



1.4.2 Manage Servers

The Manage Servers page allows you to list, update, and delete, Servers defined to the system. A user must have AdministratorRight or UpdateServerRight in order to manage Server definitions. Below is an example list of 5 Servers (*LOCAL is set by default) that had been added to MFT Internet Server. They can be managed from the Manage Servers page. It also gives you the capability to search the Server database to limit the number of Server definitions displayed. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.4.2.1 Selection Criteria

When the Selection Criteria section is expanded by clicking on the plus sign (+) you will see the available fields a search can be conducted with. This box allows you to selectively search the Server record database to limit the number of records that are displayed in the Results table. The % character is used as a wildcard character to simplify the search. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record will be returned. When you have completed the Search Criteria, click on **Search** to perform the search and create the Results table.

1.4.2.2 Results Table

The Results table will display all the servers you have defined in the system. If you click on the Server Name of an entry in the table, a detail page will be displayed that allows you to update the entry if you are authorized.

To delete a Server definition, select the check box next to the Server that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Server definitions may be deleted at one time.

If you want to refresh the Manage Servers list, you can use the Navigation box on the left portion of the screen.

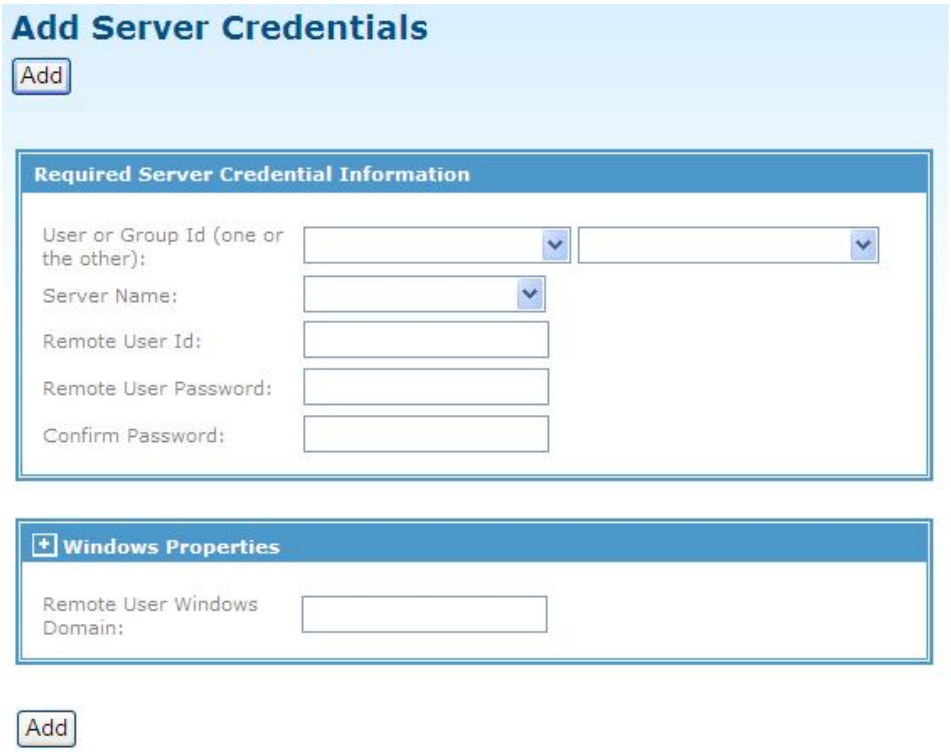
1.4.3 Server Credentials

In order to **Add Server Credentials** or **Manage Server Credentials** the user must have the AdministratorRight or UpdateServerCredentialRight. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.4.3.1 Add Server Credentials

Navigation:

Servers > Server Credentials > Add Server Credential



There are two sections on the Add Server Credentials page:

Required Server Credential Information	Defines the most important parameters needed to create a Server Credential record.
Windows Properties	Defines a Windows domain for the Server Credentials being added.

Server Credential are checked in the following order:

1) User Id
2) Group

If the user is not found in any defined Server Credentials then the Server Credentials defined in the Server definition will be used.

Upon the login the remote MFT Platform Server authentication validates that the Remote User Id is:

1) The “Administrator”
2) Part of the Local Administrators group
3) Part of the **cfadmin** or **cfbrowse** group depending on the action being attempted.

1.4.3.2 Manage Server Credentials

The user must have **AdministratorRight** or **UpdateServerCredentialRight** in order to manage Server Credential definitions. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation:

Servers > Server Credentials > Manage Server Credentials

Above is an example of 3 user credentials that had been added at an earlier date and can be managed from the Manage Server Credentials page. The page will contain a list of the first 100 defined Server Credentials. If there are more than 100 Server Credentials defined, click on "**List Next 100 >**" to access the next 100 Server Credential definitions. Use the Back button to see the previous definitions.

A listing of particular Server Credentials can be obtained by entering the search criteria for any combination of the following: Id Type, Id Name, Node Name, Remote User Id and Remote User Windows Domain. A percent sign (%) may be used as a wildcard character.

From the Manage Transfers panel, Server Credential definitions can also be updated or deleted. To update a definition, click on the Id Type of the Server Credential definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

To delete a Server Credential definition, select the check box next to the Server Credential that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Server Credential definitions may be deleted at one time.

If you want to refresh the Manage Server Credential list, you can use the Navigation box on the left portion of the screen. Click on Manage Server Credentials.

1.5 Administration

Under Administration you will apply your MFT Internet Server license key, review the various Active sessions, configure FTP and SSH Server parameters, as well as set Alerts, and global defaults for MFT Internet Server. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.5.1 System Configuration

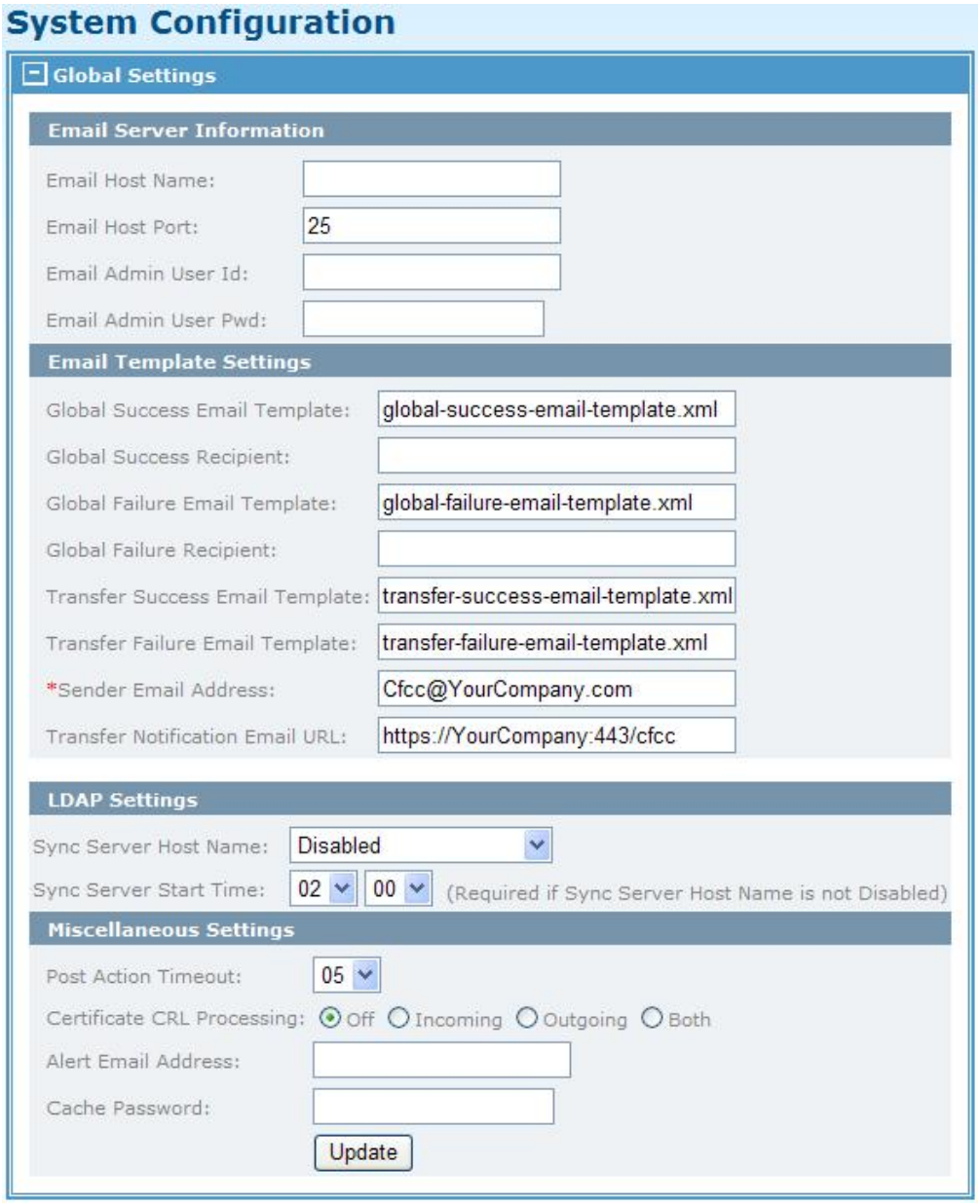
The System Configuration page sets default values for the MFT Internet Server. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

This page is broken up into ten sections, Global Settings, Password Reset, Global Password Rules, Transfer Settings, Local Settings, Global Lockout Rules, Global PGP Settings, Global FTP Settings, Global SSH Settings, and Global HTTPS Settings. (You could see a Remote Settings section if your environment is configured with multiple Internet Servers or Internet Servers pointing to the same database.).

1.5.1.1 Global Settings

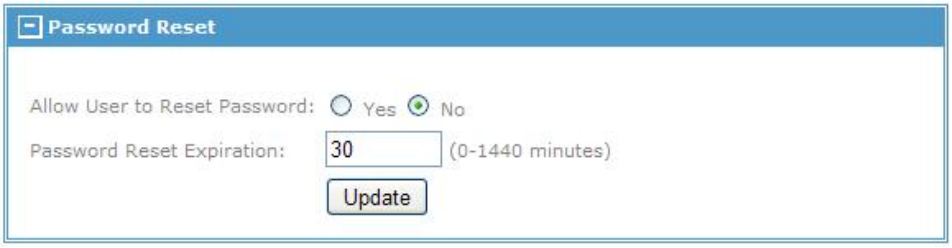
This section allows an Administrator to define settings common to all MFT Internet Servers. (See above).

Note: Global Success Email and Failed transfer notifications do not apply to AS2 transfers.



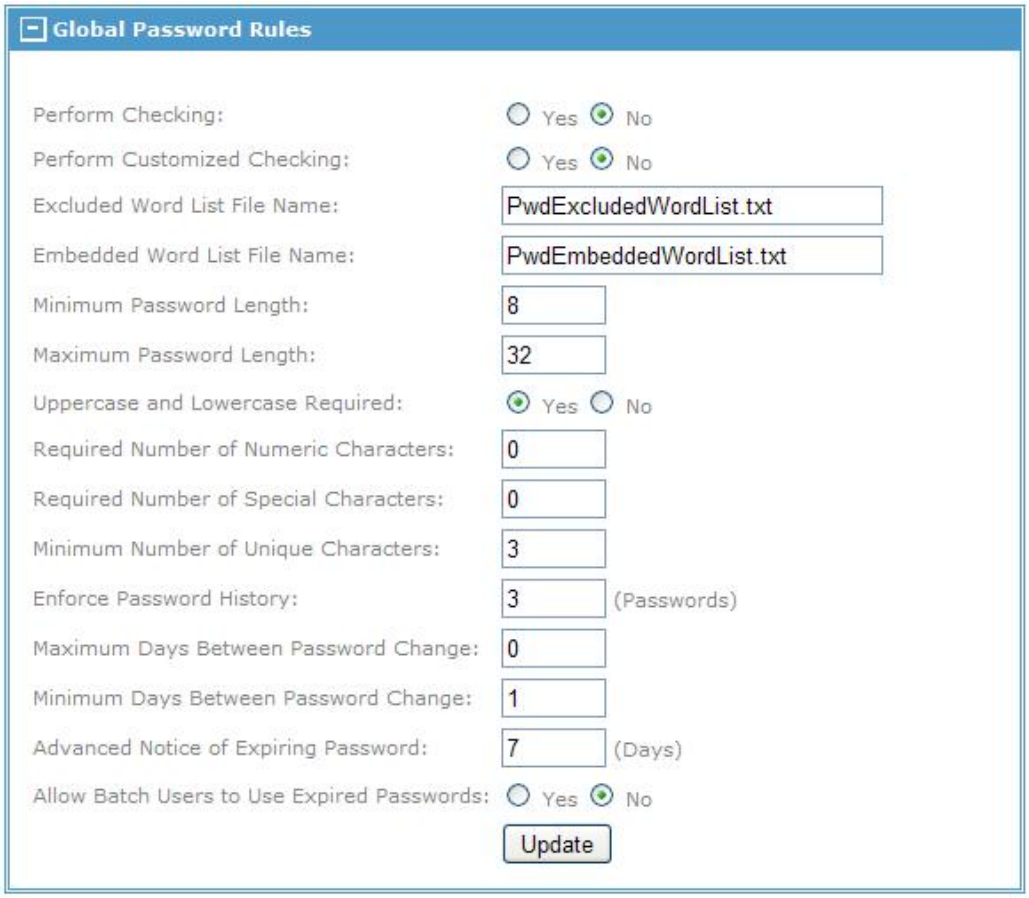
1.5.1.2 Password Reset

This section is used to define whether to allow users to reset their forgotten passwords. When an end user requests help accessing their account from the MFTIS login web page and clicks on the Reset Password link they will be prompted to type in and submit their email address associated with their account. (Email Server Information must be configured under System Configurations for this feature and an email address defined in the end users account.) They will receive an email with a link to reset their password. The password requests sent to end users will expire based on the minutes defined in the Password Reset Expiration field. The default value is 30 minutes. A value of 0 will result in the password request never expiring. Maximum value allowed is 1440 minutes.



1.5.1.3 Global Password Rules

In this section the Administrator can configure Global rules for changing and expiring passwords. *Note: These password rules would only apply to Internet Server users. Any LDAP Sync users' passwords would be controlled by LDAP.*



The default Internet Server hashing algorithm used to securely store passwords is SHA-1. Customers may optionally use the stronger SHA-256 hashing algorithm for additionally security for stored passwords using the following steps:

a. Stop Internet Server.

b. Navigate to the `<MFT_Install>`/server/webapps/cfcc/WEB-INF/ directory

c. Open the **web.xml** file using any available text editor.

d. Search for the `PasswordHashNew` parameter:

```
<context-param>
        <param-name>PasswordHashNew</param-name>
        <param-value>SHA-1</param-value>
</context-param>
```

e. Change SHA-1 to SHA-256.

f. Save the file before exiting and restart Internet Server.

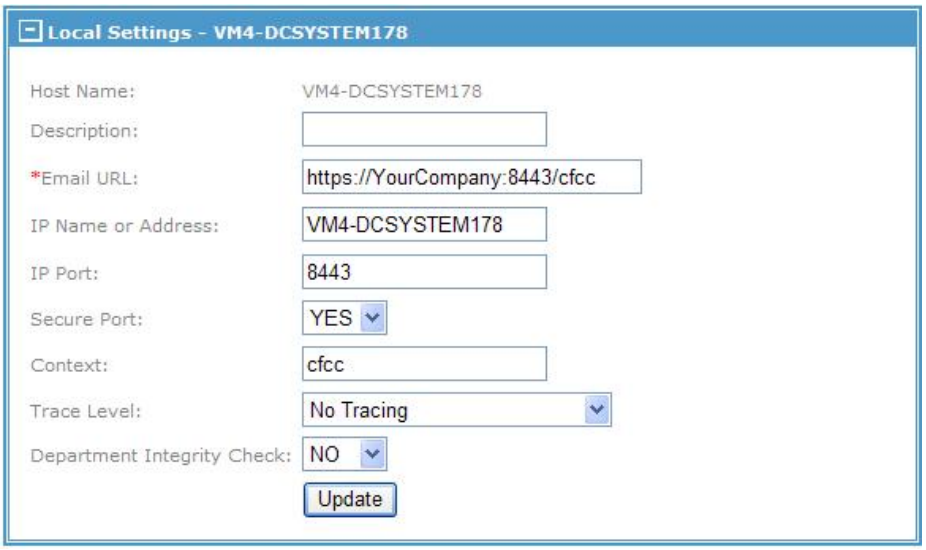
Warning: When changing between SHA-1 and SHA-256 algorithms all previous password history will be lost.

1.5.1.4 Transfer Settings

Use the **Transfer Settings** options to limit which files are transferred based on defined regular expression (REGEX) rules.

1.5.1.5 Local Settings

This section displays unique settings for the individual MFT Internet Server that are defined during the installation.



1.5.1.6 Global Lockout Rules

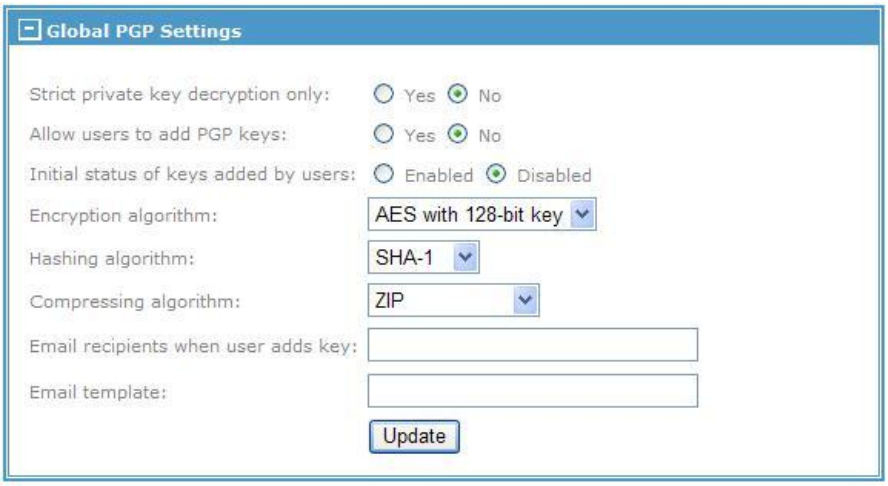
The Global Lockout Rules apply to the entire system. By setting any of the fields in the Login Failure Attempts section will require a Lock Action to be enabled. The Administrator can set either one or both Lock Actions to Yes. Note: The Send Alert Email Lock Action requires the Alert Email Address field found by expanding the Global Settings window on the System Configurations web page to be configured.

The **Failure Retention Period** time set will be reset upon a successful login for user accounts. For instance if the Login Failure Attempts for a User is set to 3 attempts and a user fails to login twice but on the third attempt is successful the failed attempts will be reset to zero. This will also occur upon the **Lock Duration** time being reached. This means if a user is locked out of the system and the **Lock Duration** time has passed the failed attempts will be reset to zero. However, this action will not occur for a System or IP **Retention Period**. To clear the attempts for these actions requires a lockout release for the System or IP Address by a Super Admin account that has been configured with a restricted IP Address to login. These user accounts are never locked out of the system. See the Lockout Management section in this manual for more details about releasing lock outs.

Note: Some care should be given when setting the **Login Failure Attempts** for the System. An acceptable number should be based on the amount of users that can access the system. The value is reached by the accumulation of User and IP failed login attempts that are being retained. A very simple example of a system lockout occurring is if the **Login Failure Attempts** for Users is set to 3 and System is set to 7 the entire system will be locked when the seventh failed attempt has occurred. (Note: The default **Failure Retention Period** for User accounts is 120 minutes.) Based on the above settings all it would take is three users to fail to access the system in a 120 minute time frame due to attempting to login with bad passwords causing the failed login attempts being retained to reach the count of 7 and the system will be locked.

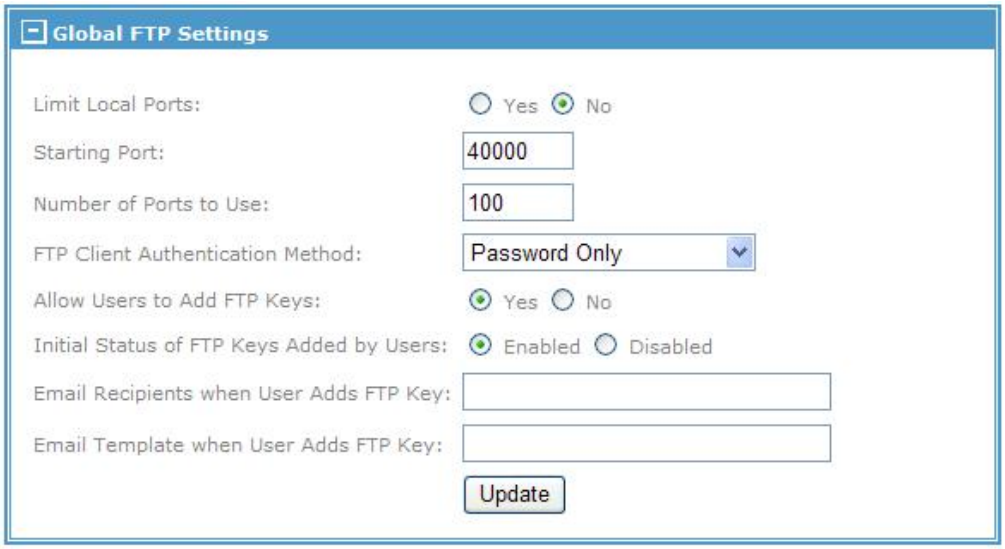
1.5.1.7 Global PGP Settings

This section displays the Global PGP settings that will be used by the MFT Server.



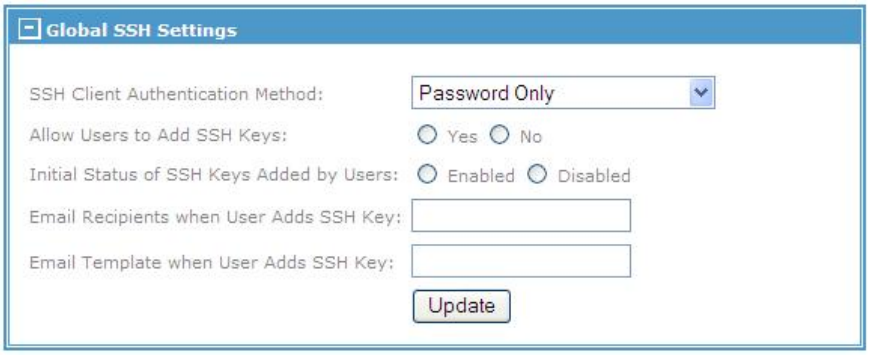
1.5.1.8 Global FTP Settings

This section displays the Global FTP settings that will be used by the MFT Server. Note: The global **FTP Client Authentication Method** can be overridden by expanding the Authentication Options window in a User's definition.



1.5.1.9 Global SSH Settings

This section displays the Global SSH settings that will be used by the MFT Server. Note: The global **SSH Client Authentication Method** settings can be overridden by expanding the Authentication Options window in a User's definition.



1.5.1.10 Global HTTPS Settings

This section displays the Global HTTPS settings that will be used by the MFT Server. Note: The global **HTTPS Client Authentication Method** can be overridden by expanding the Authentication Options window in a User's definition.

1.5.2 Transfer Servers

MFT Internet Server comes with an internal AS2 Server, an FTP Server, a Platform Server, and an SSH Server..

1.5.2.1 AS2 Server

The Configure AS2 Server and AS2 Server Status pages allow an administrator to configure, start, stop and check the status of the AS2 Server. The administrative user must have the **AdministratorRight** in order to configure and start or stop the AS2 Server. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

1.5.2.1.1 Configure AS2 Server

Before the AS2 Server can be started it must first be enabled and configured. First change the Enabled field to read **Yes**. Next both the **Receive URL** and **Async Response URL** need to be edited. Both URL's are created from information taken during the installation of MFT Internet Server and need to be edited with the correct HTTP protocol information and port. Next change the port to communicate from your internet browser to your web server using a non-ssl port number, most commonly this would be 80 but your environment might be configured differently. If your AS2 server protocol requires a Proxy server you will need to configure the Proxy Information section. If not, this may be skipped. You can also define a **Default AS2 Server ID** that would be used for incoming transfer being done with the MFT Internet Server AS2 Server or you may leave this field blank and fill it in later when setting up a Server definition. If this field is configured it can also be overridden in the Server definition. Once your changes are completed click on the **Update** button to accept them.

Note: There will be a configurable box for each Internet Server that shares the database. Within each box is an **Update** button. When you press this button, the definition changes for the Internet Server defined for this box only.

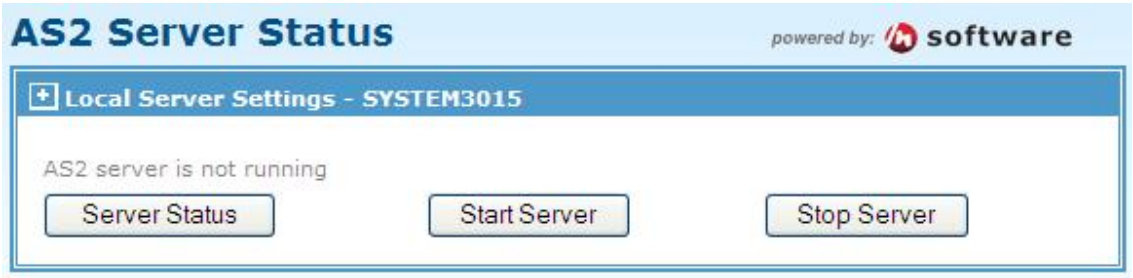
Navigation: Administration > Transfer Servers > AS2 Server > Configure AS2 Server

1.5.2.1.2AS2 Server Status

The AS2 Server Status allows you to see the current status of the AS2 Server.

To view the status of the server click on the **Server Status** button.

Navigation: Administration > Transfer Servers > AS2 Server > AS2 Server Status



1.5.2.2 FTP Server

MFT is setup with a configurable FTP/FTPS Server. This page allows you to configure both the FTP Server and the FTP SSL Server settings. The administrative user must have the **AdministratorRight** in order to configure and start or stop the FTP Server.

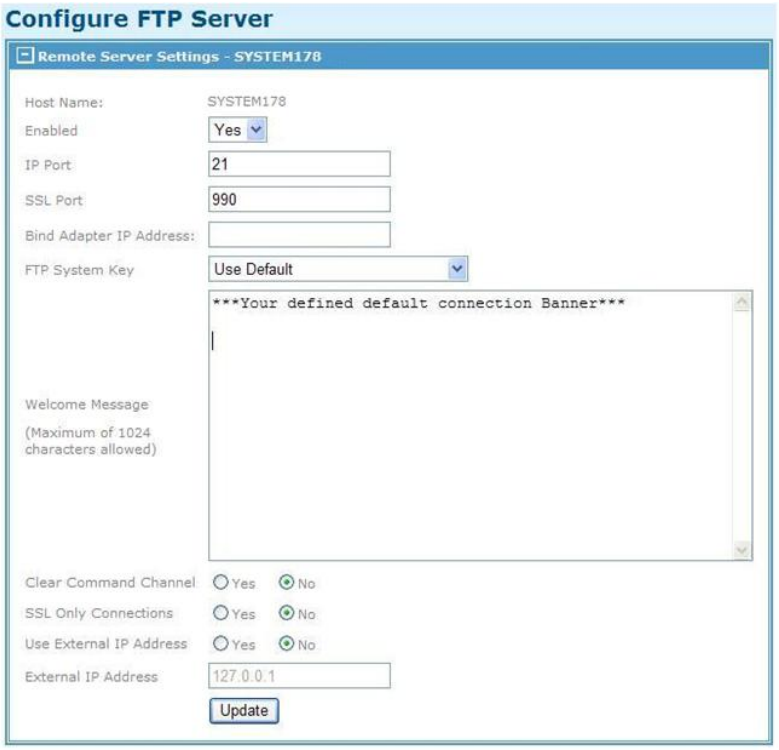
1.5.2.2.1Configure FTP Server

Before the MFT FTP Server can be started it must be enabled. By default the FTP Server is disabled. When the server is configured, click the **Update** button to save the settings. Any fields updated on the page will require the FTP Service to be restarted. See the next section named FTP Server Status for information regarding stopping and starting the service. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Note: There will be a configurable box for each Internet Server that shares the database. Within each box is an **Update** button. When you press this button, the definition changes for the Internet Server defined for this box only.

Note: It is a good idea to set the External IP Address parameter (as well as the "Use External IP Address" parameter) to the correct value since the IP Address defined on some UNIX systems defaults to 127.0.0.1.

Navigation: Administration > Transfer Servers > FTP Server > Configure FTP Server



Note: By default MFT Internet Server will request a TLS connection; however if the client does not support TLS, an SSL V3.0 connection can be negotiated. If your environment requires TLS connections, you must use a FIPS approved JAVA and put your MFTIS instance in FIPS mode.

1.5.2.2.2 FTP Server Status

This page informs the user about the status of the FTP/FTPS Server on both secure (990) and non-secure (21) ports along with the number of active sessions on those ports. The buttons will enable the user to start and stop FTP server and refresh current server status information.

Navigation: Administration > Transfer Servers > FTP Server > FTP Server Status

1.5.2.3 Platform Server

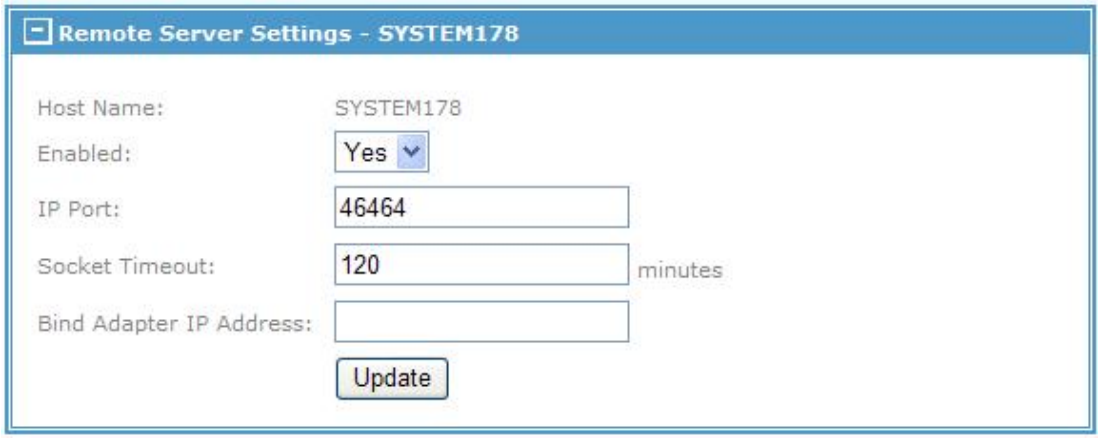
The Platform Server for MFT allows clients running MFT Platform Server on various platforms to send and receive files directly to MFT. The administrative user must have the **AdministratorRight** in order to configure, start or stop the Platform Server.

1.5.2.3.1 Configure Platform Server

Before the Platform Server can be started it must be enabled. By default the Platform Server is not enabled. The admin would navigate to the Configure Platform Server web page and change **Enable** to read Yes and either keep or edit the default port of 46464. There will be a configurable box for each MFTIS Server that is in the environment. Within each box is an **Update** button, when you press this button, the definition changes for this Internet Server Platform server only. Once this is complete you would navigate to the Platform Server Status web page and start each Platform Server you have configured. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Note: There will be a configurable box for each Internet Server that shares the database. Within each box is an **Update** button. When you press this button, the definition changes for the Internet Server defined for this box only.

Navigation: Administration > Transfer Servers > Platform Server > Configure Platform Server



1.5.2.3.2 Platform Server Status

The Platform Server Status allows you to see the current status of the Internet Server Platform Servers. Note that there is a box for each defined Internet Server.

To view the status of the server click on the Server Status button.

Navigation: Administration > Transfer Servers > Platform Server > Platform Server Status

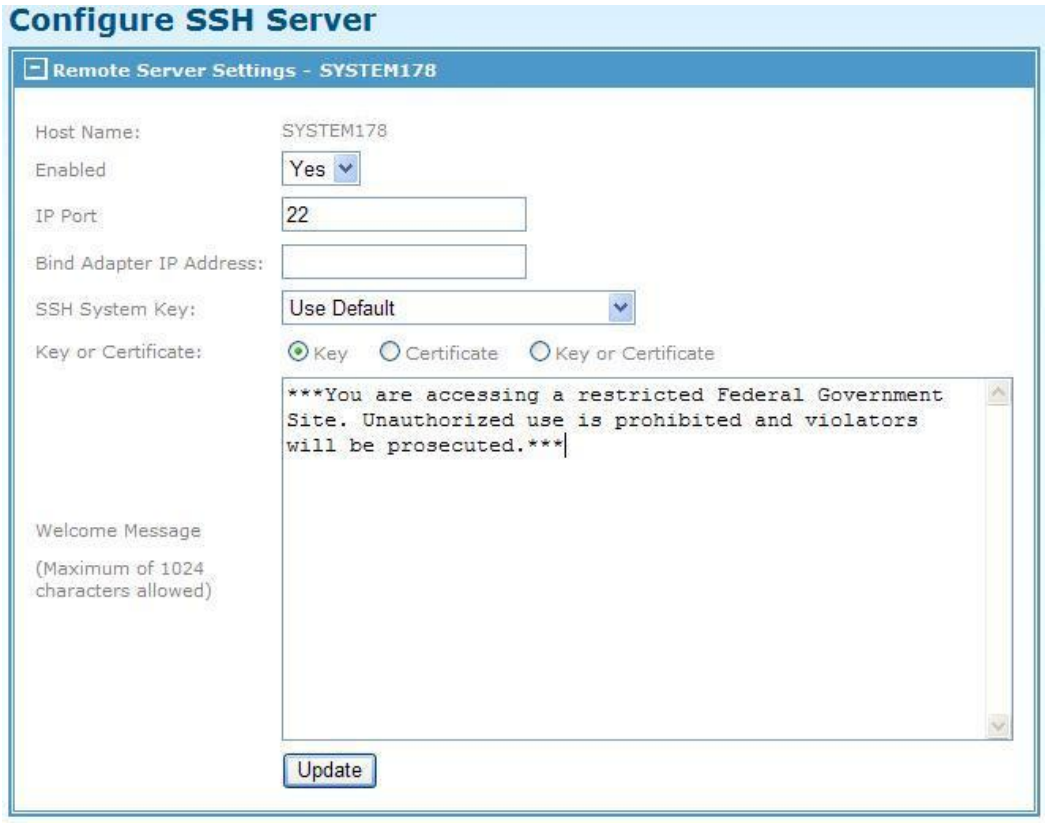
1.5.2.4 SSH Server

The Configure SSH Server and SSH Server Status pages allow an administrator to configure, start, stop and check the status of the MFT SSH Server. The administrative user must have the **AdministratorRight** in order to configure and start or stop the SSH Server.

1.5.2.4.1Configure SSH Server

Before the MFT Platform Server Internet Server SSH server can be started it must first be configured and enabled. There will be a configurable box for each Internet Server that has been defined. Within each box is an **Update** button, when you press this button the definition changes for the Internet Server defined by this box only. Two types of SSH keystores are supported: DSA and RSA. By default Internet Server comes with a working DSA keystore (Primary Keystore) that will work and all the admin has to do is set the Enabled field to read “Yes”. You should only update the keystore if you want to create a keystore specifically for your installation. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation: Administration > Transfer Servers > SSH Server > Configure SSH Server



Note: Any changes to your Welcome Message will require the SSH Server to be restarted. Please see the next section for those instructions.

1.5.2.4.2SSH Server Status

The SSH Server Status allows you to see the current status of the Internet Server SSH Servers. Note that there is a box for each defined Internet Server as well as allow the administrator to Stop and start the SSH Servers. These boxes contain the status information about the SSH server on that Internet Server.

Navigation: Administration > Transfer Servers > SSH Server > SSH Server Status

Note: SSH zero byte file transfers are not supported at this time and will error out.

1.5.3 Keys

MFT Internet Server can store FTP, PGP, SSH, HTTPS Public Keys, and Trusted Certificates as well as create and store AS2, FTP, PGP and SSH System Keys (a.k.a Secret or Private Key), in the database. A Super Administrator (user that has **AdministratorRight** and not a member of a department) can Add and Manage all keys in the system. Using special user rights the administration can be assigned to different users to assist with this responsibility. The table below lists the rights and gives a brief description:

User Right	Description
UpdateAS2SystemKeyRight	Allows a user to Create/Manage AS2 System Keys
UpdatePGPKeyRight	Allows a user to Add/Manage PGP Public Keys
UpdatePGPSystemKeyRight	Allows a user to Create/Manage PGP System Keys
UpdatePublicKeyRight	Allows a user to Add/Manage FTP, SSH, HTTPS Public Keys, and Trusted Certificates
UpdateSystemKeyRight	Allows a user to Create/Manage FTP and SSH System Keys

1.5.3.1 AS2 System Keys

1.5.3.1.1 Create AS2 Keys

Navigation: Administration > Keys > AS2 System Keys > Create AS2 Key

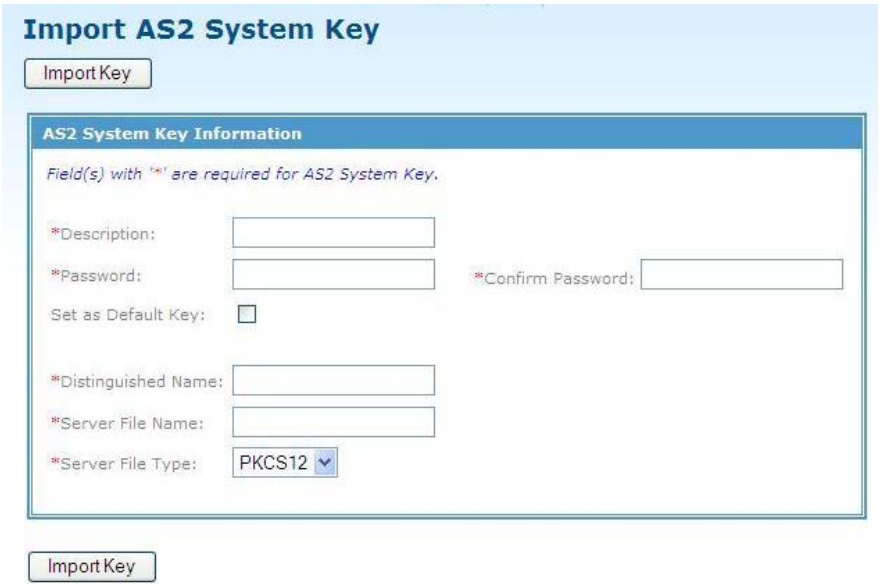
Below is an Example of an AS2 System Key being created:

Fill in the necessary parameters and click on the **Create Key** button to create the AS2 System Key.

1.5.3.1.2 Import AS2 Keys

The Import AS2 System Key page allows you to import an AS2 System Key from a PKCS12 file or from a JAVA keystore (JKS file).

Navigation: Administration > Keys > AS2 System Keys > Import AS2 Key

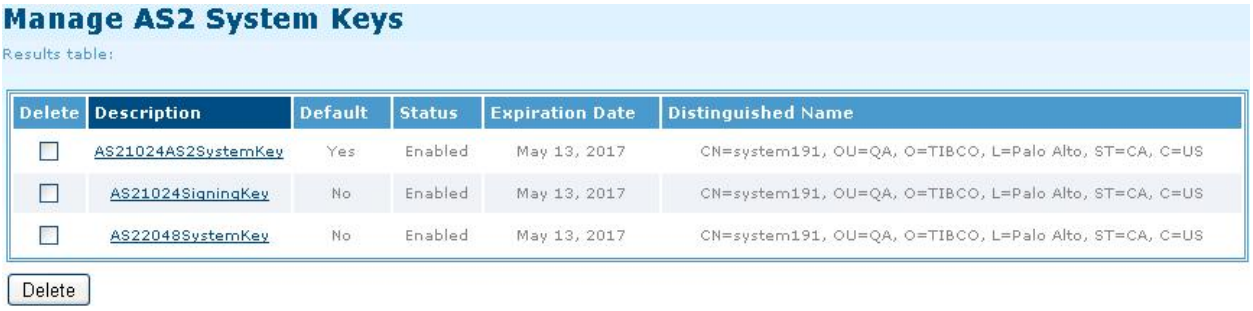


Fill in the necessary parameters and click on the **Import Key** button to create the AS2 System Key.<MFT_Install>

1.5.3.1.3 Manage AS2 Keys

This screen shows the AS2 keys available. You may have one AS2 key or there may be several. From this screen an administrator can delete keys.

Navigation: Administration > Keys > AS2 System Keys > Manage AS2 Keys



By clicking on one of the links under **Description** of a particular key you will see the detailed information about the key, below see the information as a result of clicking on AS22048SystemKey from the above screenshot:

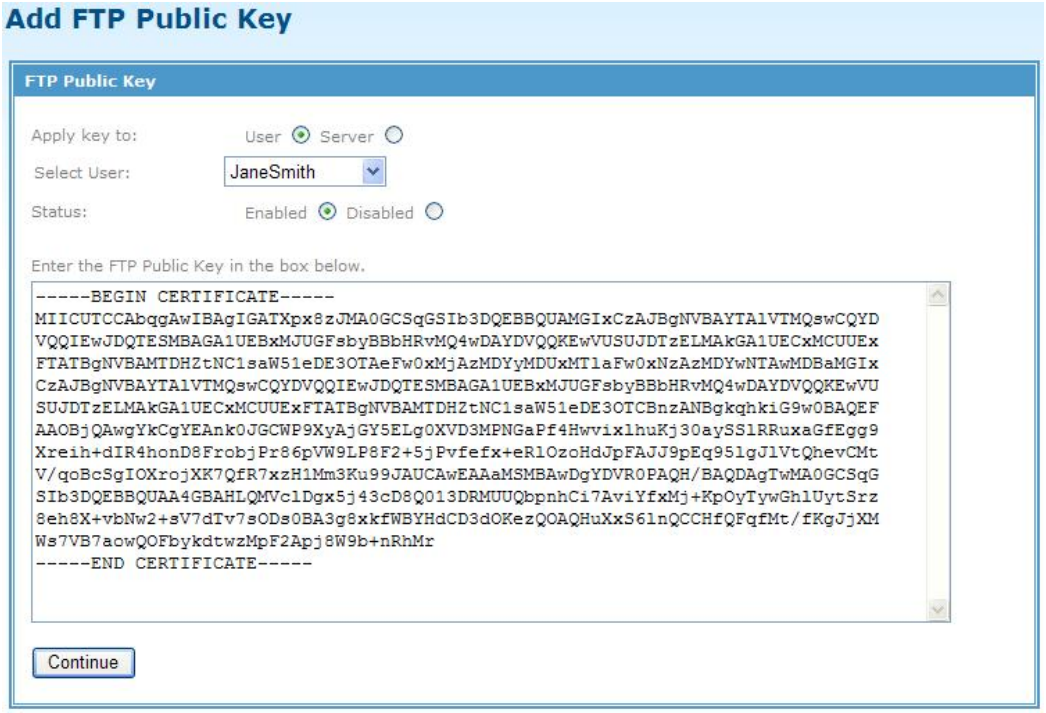
The Admin can either make this AS2 key the new default key or they can disable the key.

1.5.3.2 FTP Public Keys

The FTP Public keys are associated with a MFT User or MFT Server definition.

1.5.3.2.1 Add FTP Public Keys

Navigation: Administration > Keys > FTP Public Keys > Add FTP Keys



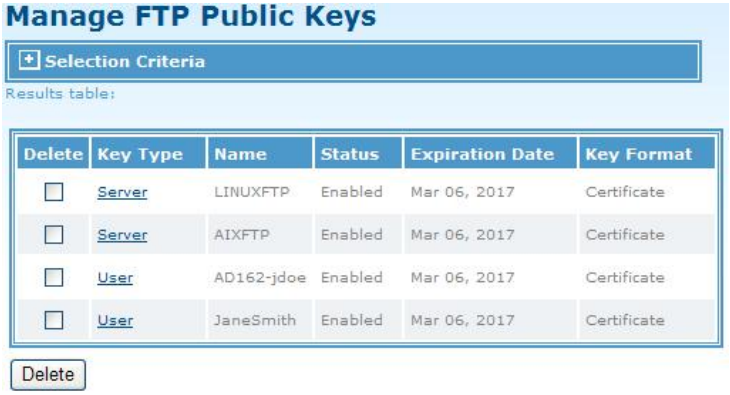
When you have entered data in all of the fields, press the **Continue** button to add the public key.

Note: You cannot add a Public Key for a User or Server that already has a Public Key associated with it. Use the Manage FTP Keys web page to update or replace a key for a user or server.

1.5.3.2.2 Manage FTP Keys

Under the Manage FTP Keys section, FTP Public keys are listed. Please refer to the on line Help screen for a detailed description for each field available to be configured on this web page.

Navigation: Administration > Keys > FTP Public Keys > Manage FTP Keys



The above screen shot shows the Manage FTP Public Keys web page with 4keys that have been added to the database prior for this example. This page can contain a list of the first 100 defined FTP keys. If there are more than 100 FTP Public keys defined, click on “List Next 100 >” to access the next 100 key definitions. Use the Back button to see the previous definitions.

A list of keys can be obtained by entering the search criteria for any combination of the following: User Keys/Server Keys, Enabled/Disabled keys, or simply by putting in the name of the particular FTP public key you want to see. A percent sign (%) may be used as a wildcard character.

To update a key definition, click on the Key Type of the FTP Public Key definition that you would like to change. Once the changes are made, click on the Update button to update the definition.

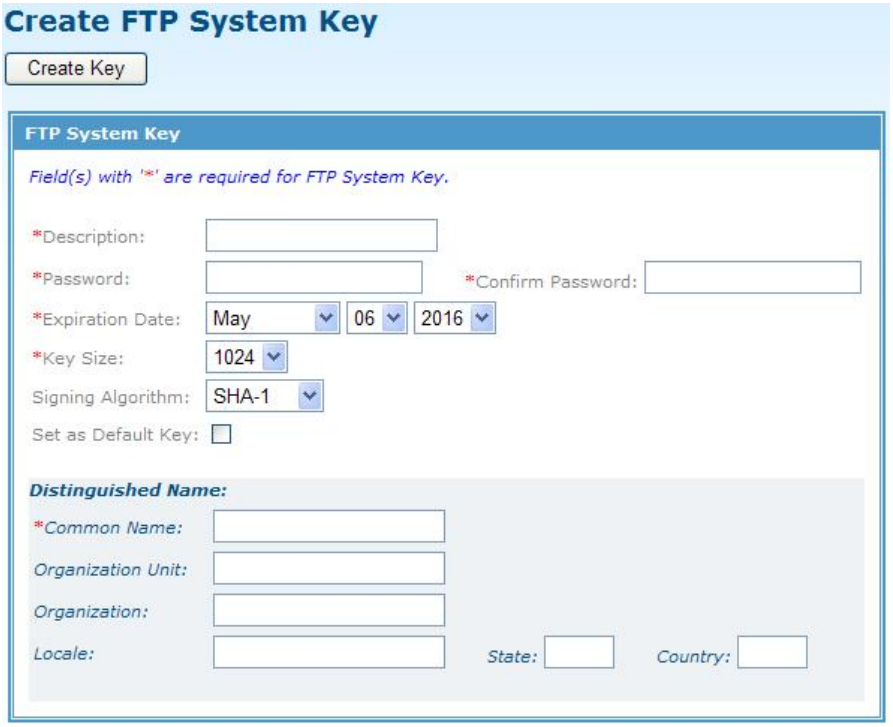
To delete a key definition, select the check box next to the key that you wish to delete and click on the Delete button at the bottom of the panel. Multiple key definitions may be deleted at one time.

To refresh the Manage FTP Public Keys list, you can use the Navigation box on the left portion of the screen.

1.5.3.3 FTP System Keys

1.5.3.3.1 Create FTP System Keys

Navigation: Administration > Keys > FTP System Keys > Create FTP Key



When the necessary parameters are defined, the user should click on the **Continue** button to add the FTP System Key to the MFT database.

1.5.3.3.2 Import FTP System Key

The Import FTP System Key page allows you to import an FTP System Key from a JAVA keystore (JKS file).

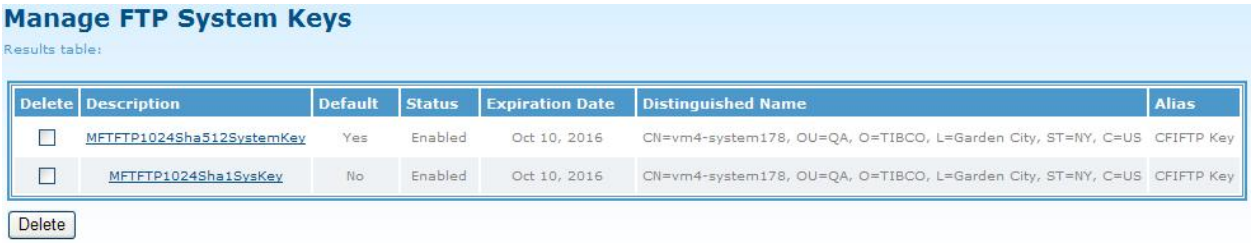
Navigation: Administration > Keys > FTP System Keys > Import FTP Key

Fill in the necessary parameters and click on the **Import Key** button to create the FTP System Key.

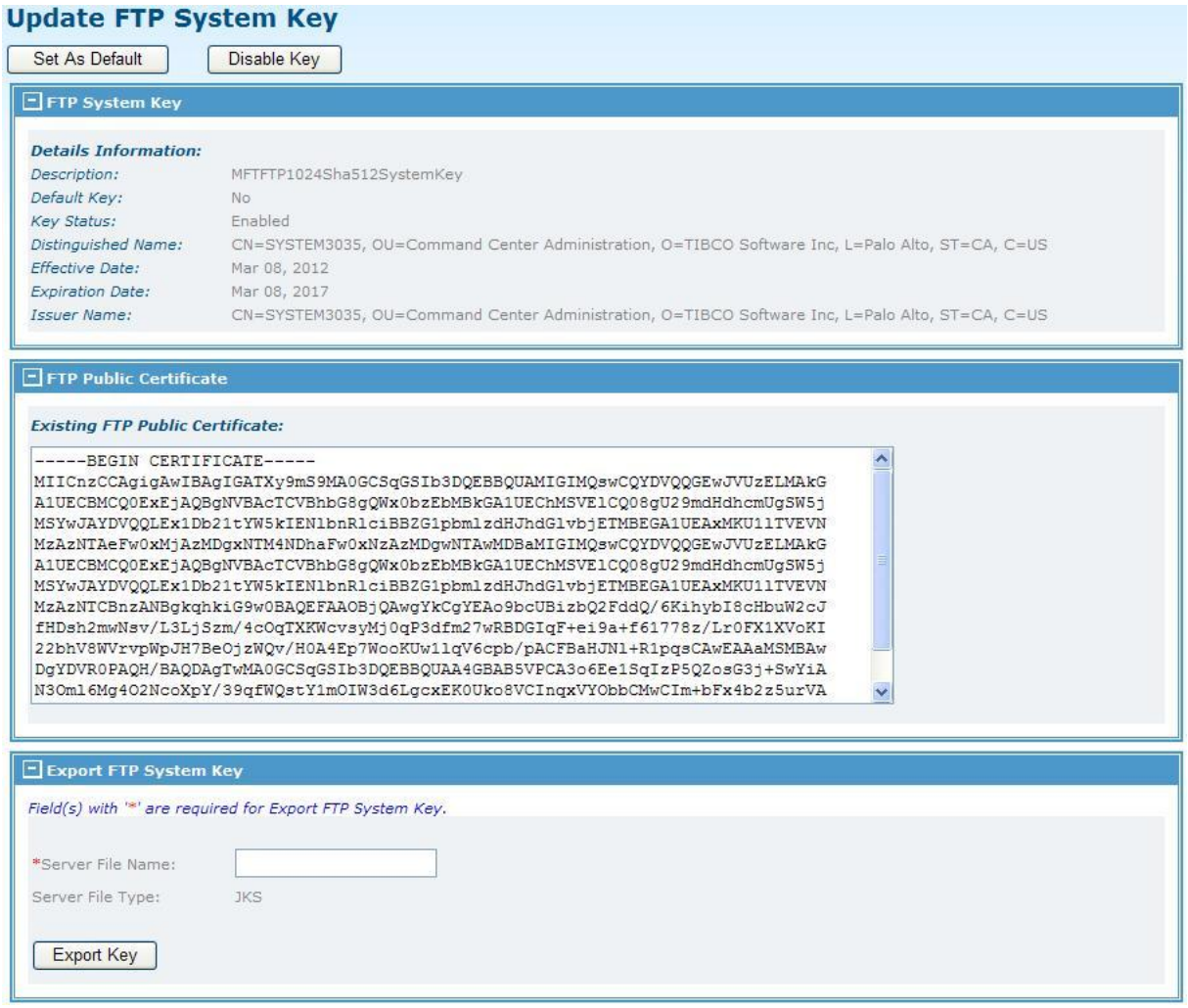
1.5.3.3.3 Manage FTP System Keys

This screen shows the FTP System Keys available. From this screen an administrator can delete keys by placing a check in the box under the Delete column next to the key they want to delete and clicking on the **Delete** button. They will be asked to confirm the deletion.

Navigation: Administration > Keys > FTP System Keys > Manage FTP Keys



By clicking on the **Description** of a particular key it will allow the administrator to see the detailed information about the key, below is the information that is displayed as a result of clicking on MFTFTP1024Sha512SystemKey from the above screen shot (All 3 sections have been expanded):



From this web page the administrator can disable the key, he can Display/Replace the FTP Public key by pasting a new FTP Public key in the box provided, or he may export the system key to a .jks file type. If only a file name is provided for the exported file the default location the file will be written is <MFTIS_Install>/cfcc/ftp/tmp.

1.5.3.4 PGP Public Keys

The PGP Public keys are associated with a MFT User or MFT Server definition.

1.5.3.4.1 Add PGP Public Keys

Navigation: Administration > Keys > PGP Public Keys > Add PGP Keys

When you have entered data in all of the fields, press the **Continue** button to add the public key.

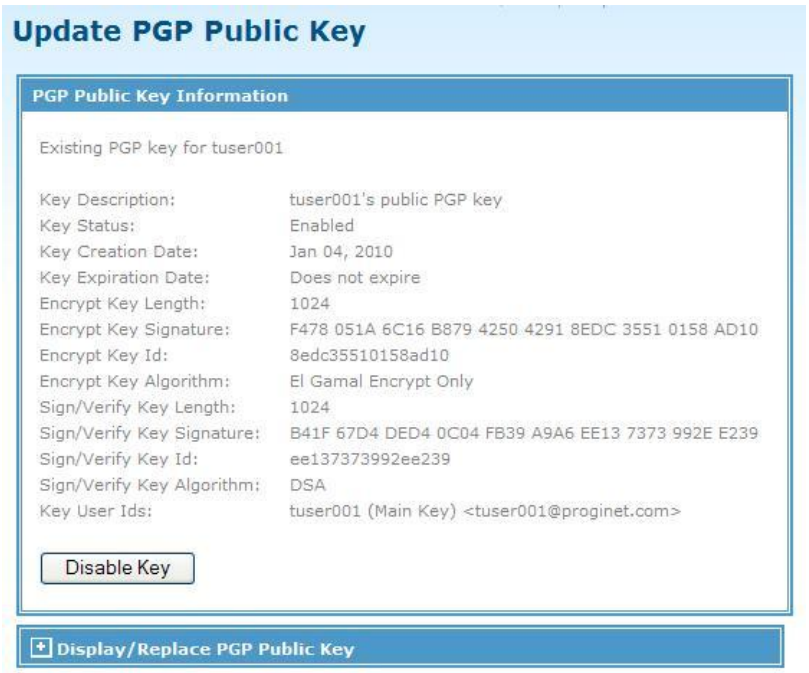
Note: You cannot add a Public Key for a User or Server that already has a Public Key associated with it. Use the Manage PGP Keys web page to update or replace a key for a user or server.

1.5.3.4.2 Manage PGP Public Keys

This screen shows the PGP Public Keys available. From this screen the administrator can delete keys by placing a check in the box under the Delete column next to the key they want to delete and clicking on the **Delete** button. They will be asked to confirm the deletion.

Navigation: Management > Keys > PGP Public Keys > Manage PGP Keys

By clicking on the **Key Type** of a particular key would allow the Administrator to see the detailed information about the key, below is the information that is displayed as a result of clicking on User for tuser001from the above screen shot:

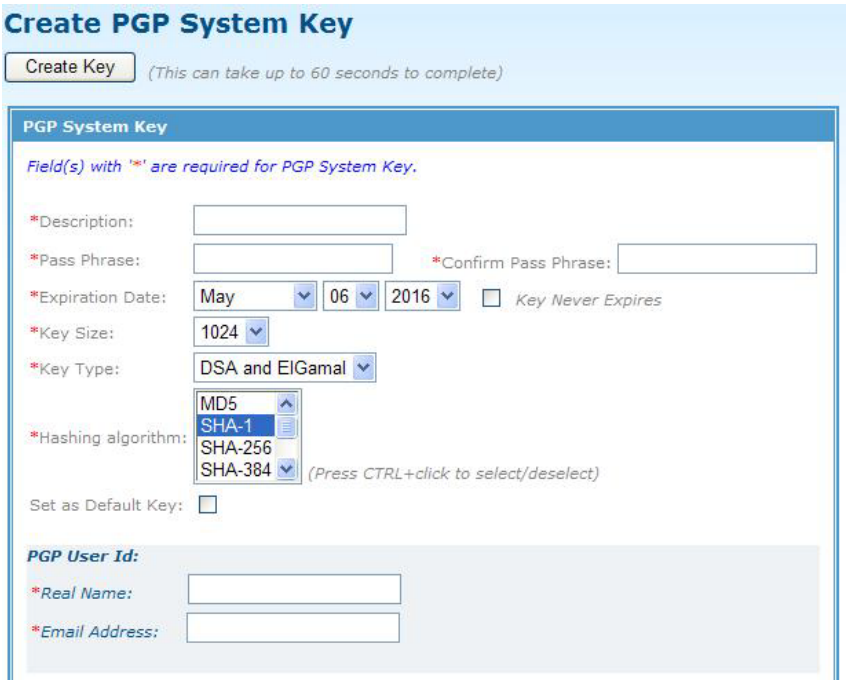


The administrator can either disable the key or he can expand the Display/Replace PGP Public key section to paste a new PGP Public key in for this user.

1.5.3.5 PGP System Keys

1.5.3.5.1 Create PGP System Keys

Navigation: Administration > Keys > PGP System Keys > Create PGP Keys



When the necessary parameters are defined, the user should click on the **Continue** button to add the PGP System Key to the MFT database.

1.5.3.6 SSH Public Keys

The SSH Public keys are associated with a MFT User or MFT Server definition.

1.5.3.6.1 Add SSH Public Keys

Navigation: Administration > Keys > SSH Public Keys > Add SSH Keys

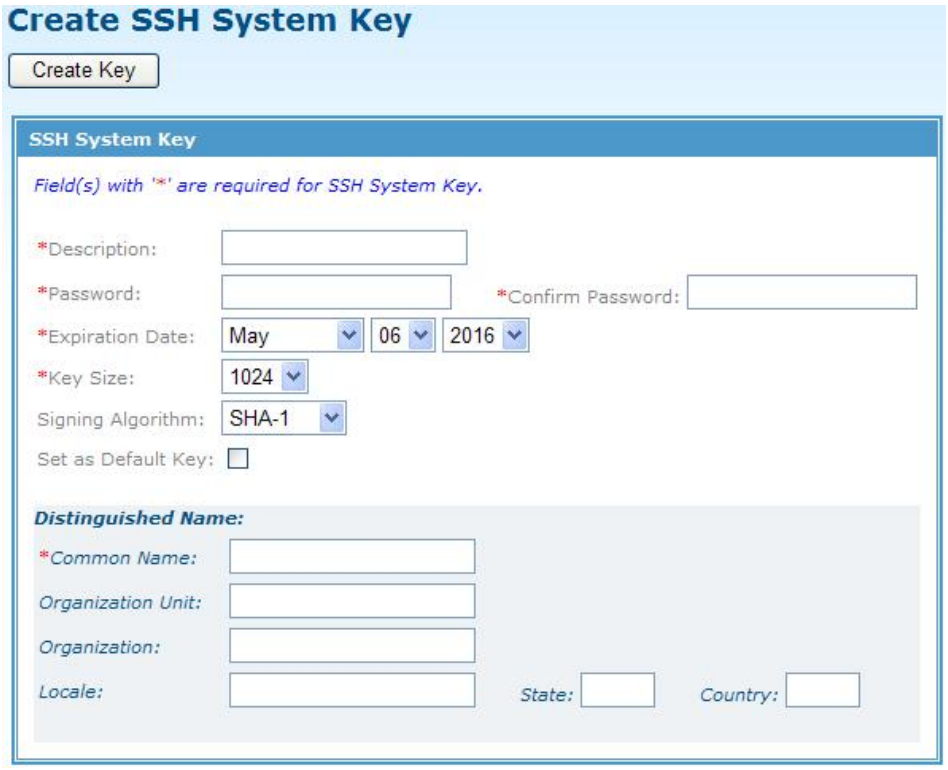
When you have entered data in all of the fields, press the **Continue** button to add the public key.

Note: You cannot add a Public Key for a User or Server that already has a Public Key associated with it. Use the Manage SSH Keys web page to update or replace a key for a user or server.

1.5.3.7 SSH System Keys

1.5.3.7.1 Create SSH System Keys

Navigation: Administration > Keys > SSH System Keys > Create SSH Key



When you have entered data in all of the fields, press the **Continue** button to add the public key.

Note: You cannot add a Public Key for a User or Server that already has a Public Key associated with it. Use the Manage SSH Keys web page to update or replace a key for a user or server.

When the necessary parameters are defined, the user should click on the **Continue** button to add the SSH System Key to the MFT database.

1.5.3.7.2 Import SSH System Keys

Navigation: Administration > Keys > SSH System Keys > Import SSH Keys

1.5.3.7.3 Manage SSH System Keys

This screen shows the SSH Public Keys available. From this screen the administrator can delete keys by placing a check in the box under the Delete column next to the key they want to delete and clicking on the **Delete** button. They will be asked to confirm the deletion.

Navigation: Management > Keys > SSH Public Keys > Manage SSH Keys

Clicking on the **Description** of a particular key would allow the Administrator to see the detailed information about the key, below is the information that is displayed as a result of clicking on one of the Description links from the above screen shot:

The administrator can either disable the key or he can expand the Display/Replace SSH Public key section to paste a new SSH Public key in for this user.

1.5.3.8 HTTPS Public Keys

The HTTPS Public keys are associated with user accounts.

1.5.3.8.1 Add HTTPS Public Key

Navigation: Administration > Keys > HTTPS Public Keys > Add HTTPS Key

Select a User from the drop down list that will be linked to this certificate. Select whether the certificate will be enabled or disabled at this time. Paste the Base64 version of the certificate into the space prvided. Be sure to include the BEGIN and END statements as in the example below:

-----BEGIN CERTIFICATE-----

.....HTTPS key information.....
.....HTTPS key information.....

-----END CERTIFICATE-----

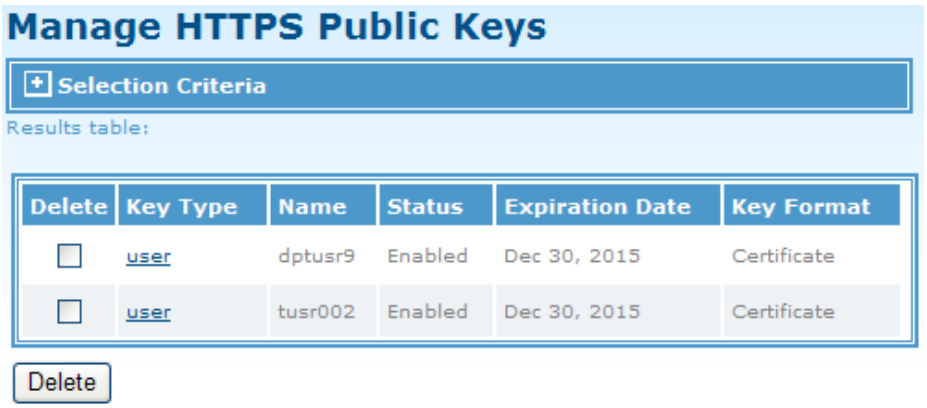
When you have completed adding all the data needed click on the **Continue** button. You will be presented with an Add HTTPS Public Key Confirmation page, click the **Continue** button to add the certificate.

Note: One certificate is associated with one user account at a time. To replace a certificate used by a user account navaigate to the Manage HTTPS Keys web page.

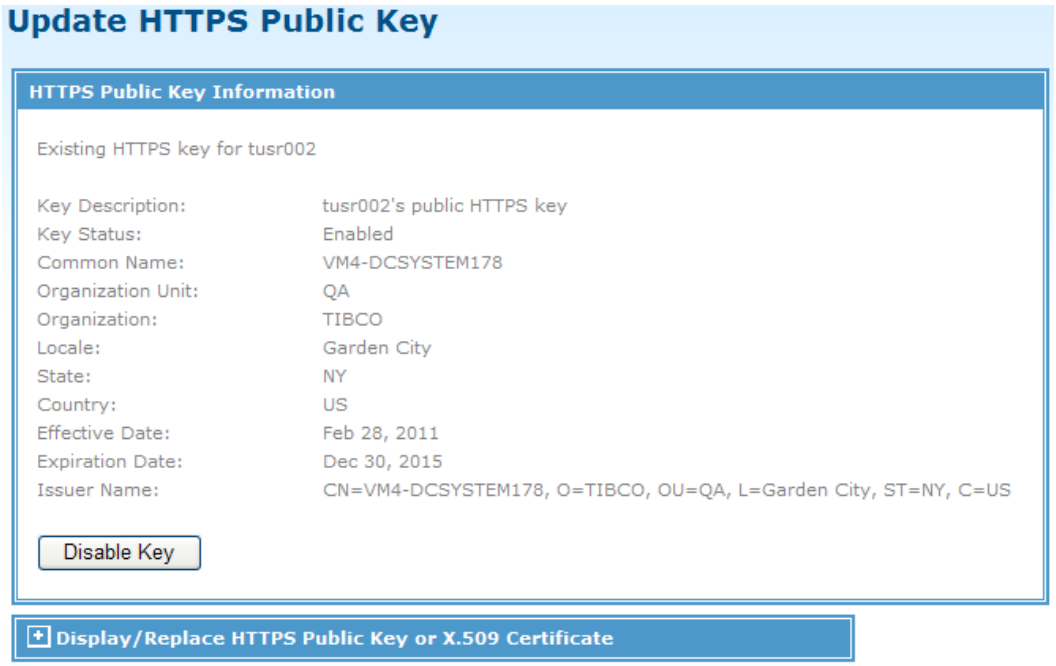
1.5.3.8.2 Manage HTTPS Keys

This screen shows the HTTPS Public Keys available. From this screen the administrator can delete keys by placing a check in the box under the Delete column next to the key they want to delete and clicking on the **Delete** button. They will be asked to confirm the deletion.

Navigation: Administration > Keys > HTTPS Public Keys > Manage HTTPS Keys



Click the link under **Key Type** to display the **Update HTTPS Public Key** page. You can use this page to view key information and to replace the X.509 Certificate for this user.



By expanding the Display/Replace HTTPS Public Key or X.509 Certificate box you can paste a new Key or Certificate.

1.5.3.9 Trusted Certificates

Trusted Certificates are a more flexible way to define X.509 certificates for both SFTP(SSH) and FTPS transfers. Typically a CA (Certificate Authority) Certificates will be added as a Trusted Certificate(s) to MFTIS. When Certificate Authentication is turned on for your MFTIS SSH Server through the Management>System Servers>SSH Server>Configure SSH Server web page and an SSL negotiation is performed any certificate signed by the Trusted Certificate will be accepted. Then the Distinguished Name of the certificate will be matched against the “Certificate DN” in the User’s definition to associate the certificate with a user.

Note: If you want to monitor a CRL for revoked certificates. You would need to save the CRL list in to `<MFT_Install>\<context>\ftp\crl` directory. Then navigate to Management>System Configurations and expand the Global Settings box. Here you would set the Certificate CRL Processing. All Outgoing CRL Processing is for Server certificate authentication. Incoming is for either User or Server authentication.

Validation of certificates is done:

Incoming: If a certificate is assigned to a user/server the Trusted Certificate is not checked. In addition MFTIS will check:

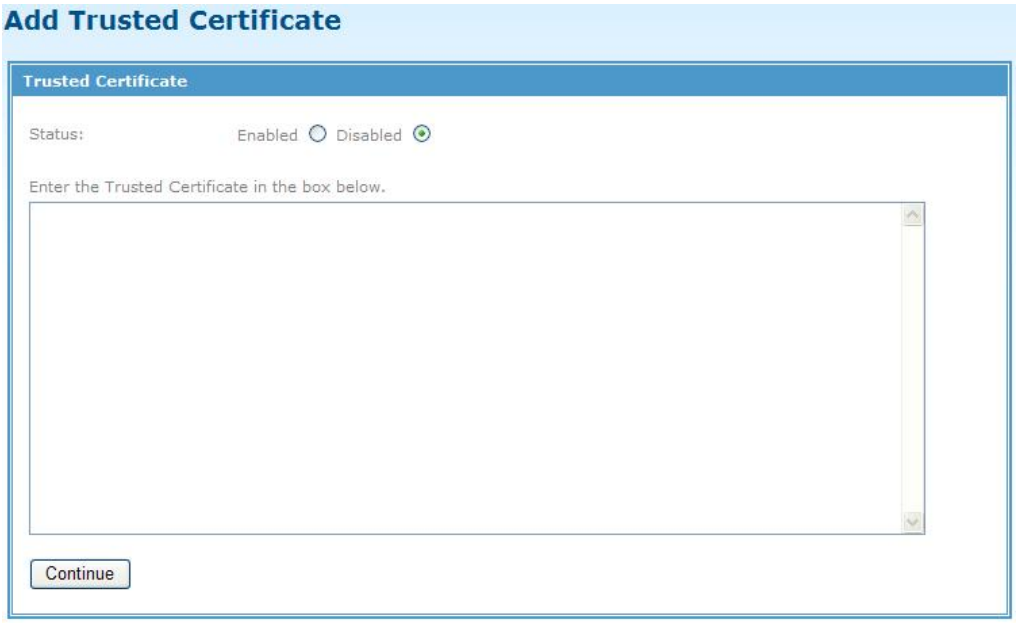
1. If the certificate is enabled
2. Check the CRL if Certificate CRL Processing is enabled.

If no certificate is found assigned to a user/server then the Trusted Certificates will be used for validation, performing the following tasks:

1. Verify the certificate is signed by one of the Trusted Certificates in the MFTIS database
2. Check the CRL if Certificate CRL Processing is enabled.
3. Validate the DN extracted from the certificate against the Certificate DN parameter found in the User’s definition.

1.5.3.9.1 Add Trusted Certificates

Navigation: Administration > Keys > Trusted Certificates > Add Trusted Certificate



When you have entered data in all of the fields, press the **Continue** button. You will be presented with an Add Trusted Certificate Confirmation page, click the **Continue** button to add the certificate.

Once you have added the Trusted Certificate to the system and you have signed certificates generated by that Trusted Certificate for an end user defined in MFT you will want to navigate to the user's configurations and fill in the **Certificate DN** for that user.

1.5.3.9.2 Manage Trusted Certificates

This screen shows the Trusted Certificates available. From this screen the administrator can delete certificates by placing a check in the box under the Delete column next to the certificate they want to delete and clicking on the **Delete** button. They will be asked to confirm the deletion.

Navigation: Administration > Keys > Trusted Certificates > Manage Trusted Certificate

When you click on the **Certificate Type** of a certificate listed it will allow you to see the detailed information about that certificate.

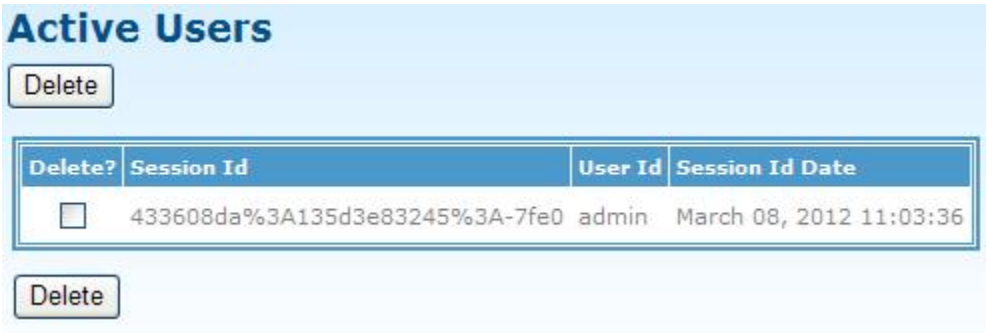
From the details page a certificate can be disabled/enabled and displayed by expanding the Display Trusted Certificate window.

1.5.4 Activity

To view the active sessions and checkpoints, select Management and Activity. The administrative user must have the **AdministratorRight** or **UpdateSessionRight** in order to view the sessions.

1.5.4.1 Active Users

Navigation: Administration > Activity > Active Users



This page displays all the active sessions in the system. In our example above you can see the admin's session currently running.

To delete a user's session, select the check box next to the session that you wish to delete and click on the Delete button at the bottom of the panel. Multiple sessions may be deleted at one time.

1.5.4.2 Internet Checkpoints

The Internet Checkpoints list contains checkpoints for all transfers done using Platform Server, the Internet Transfer Client, and the Desktop Client. The user must have **AdministratorRight** in order to manage Checkpoints.

Navigation:

Administration > Activity > Internet Checkpoints

This will take you to a page containing a section for Selection Criteria and a list of the first 100 Checkpoints. If there are more than 100 Checkpoints, click on "List Next 100 >" to access the next 100 Checkpoints. Use the Back button to see the previous Checkpoints.

A listing of particular Checkpoints can be obtained by entering the search criteria for any combination of the following: File Id, User Id, Client File Name, Node Name, Server File Name, Transaction Id and Proxy Transaction Id. A percent sign (%) may be used as a wildcard character.

To delete a Checkpoint, select the check box next to the Checkpoint that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Checkpoints may be deleted at one time.

1.5.5 License

The administrative user must have the **AdministratorRight** in order to add or manage the license keys.

1.5.5.1 Add License Key

Navigation: Administration > License > Add License Key

1.5.5.2 Manage License Keys

Navigation: Administration > License > Manage License Keys

This will take you to a page containing a list of all the keys that have been applied to MFT Internet Server.

To delete a License Key from the Manage License Keys panel select the check box next to the License Key that you wish to delete and click on the Delete button at the bottom of the panel. Multiple License Keys may be deleted at one time.

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

1.5.5.3 Host Information

Selecting Management, License and Host Information will take you to the Host Information page.

Navigation: Administration > License > Host Information

This will display the MFT Internet Server Host Name.

1.5.6 Authenticators

MFT Users can be added to the MFT database manually, through the Java Command Line Utility, and by authenticating to an LDAP server such as Active Directory. MFT provides easy integration with LDAP servers which is configured from the MFT Internet Server Add Authenticartor web page and tested from the Manage Authenticator web page. By default the LDAP user's Login id, Full Name, Email Address (optional), and Telephone Number (optional) are pulled into the MFT Internet Server database. In addition to controlling user's details being pulled from the LDAP server the Administrator can optionally setup what MFT Internet Server rights are assigned to those LDAP users.

To add and manage LDAP authenticators a user must have the MFTIS **AdministratorRight** assigned to them in the system.

To allow MFTIS to Authenticate and Synchronize with an LDAP server you must have the following items on the LDAP server configured:

1. You must know the Host information such as the IP and Port of the LDAP server(s) you will be authenticating to.
2. You must know the Bind User DN and Password.
3. You must have a container such as an OU, or group which contains the specific users to be sync'd with the MFT database; for example **OU=MFT Users** would contain all users which will sync with MFT. (See Figure 2 below.)
4. You must know the User Base DN and Group Base DN where the Sync Group is located.

Note: When using non-AD servers; groups must contain the object class groupofUniqueNames, and users must contain the object class inetOrgPerson.

Example Active Directory setup:

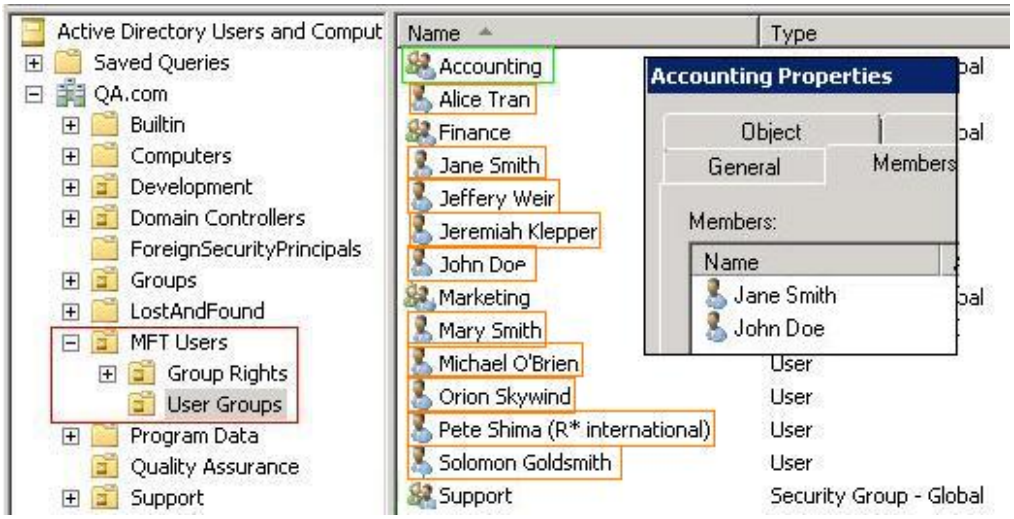


Figure 2

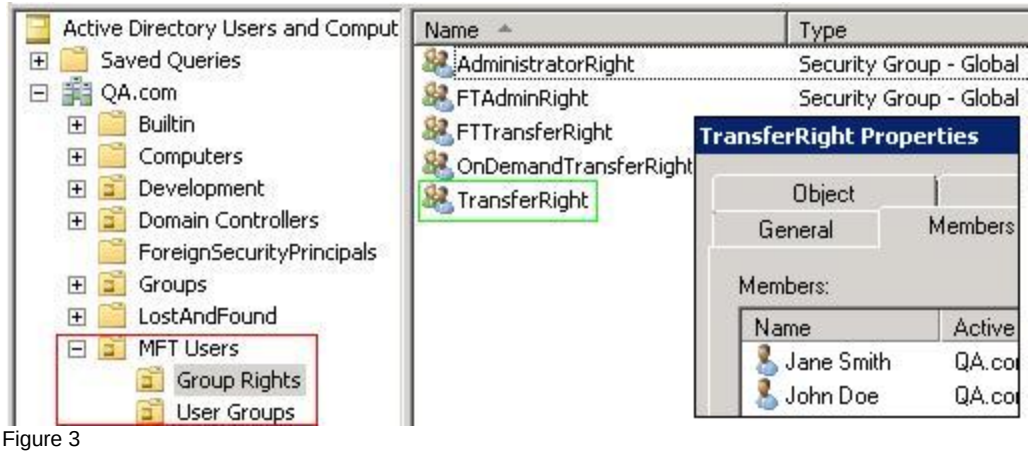


Figure 3

1.5.6.1 Add Authenticator

In order to synchronize the MFT database through LDAP, you must configure an LDAP authenticator. On the Add Authenticator page you will see the Authenticator Properties form. The first section that needs to be configured is **Authenticator**.

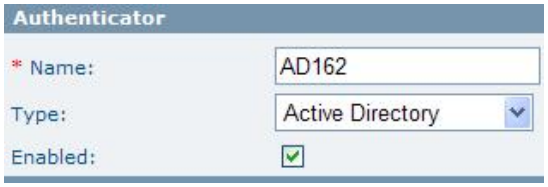


Figure 4

Note: It is recommended to use a short name for the Authenticator. When LDAP user ids are synchronized they will be represented in the MFT Database in the format of xxxxx-userid where xxxxx is the Authenticator Name. End users will not need this portion of the userid to login to the system. Example: John Doe (jdoe) would login with jdoe and not AD162-jdoe.

The table below defines the parameters for the section.

Parameter	Definition
Name	This is the unique name of the LDAP Authenticator in MFT and is used as the prefix to the user id followed by a dash when it is pulled in from the LDAP server. Ex. LDAPServer-john.doe Warning: This field cannot be modified later.
Type	The type of directory where LDAP is pulling the user and role credentials from such as Active Directory, eDirectory, Sun Directory Server, Tivoli, and others.
Enabled	Enables or Disables this LDAP Authenticator. If this box is disabled all users connected to this LDAP server will no longer be able to connect to the MFT server. Disabled users will lose “TransferRight” and show LDAP status as “Inactive” on the User Properties page in MFTCC or MFTIS.

The next section is **LDAP Connectivity** which defines the parameters necessary to connect to the directory server and pull in the user and role information for synchronizing.

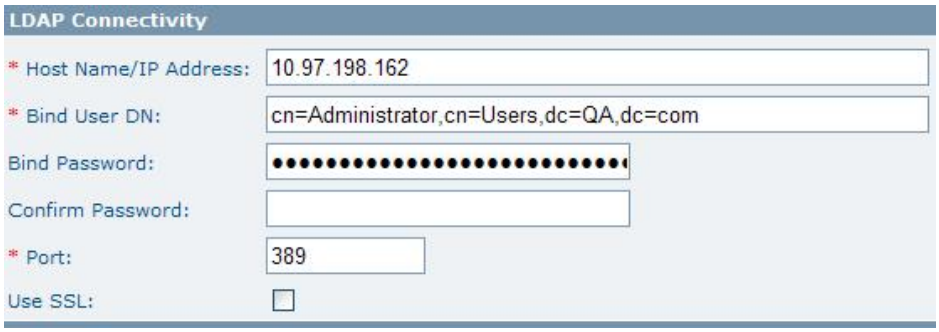


Figure 5

Parameter	Definition
Host Name/IP Address	Host Name or IP Address of the LDAP server.
Bind User DN	The distinguished name (DN) required for authenticating to the LDAP Server.
Bind Password	The password associated with the defined Bind User.
Confirm Password	Confirmation for the password associated with the defined Bind User.
Port	The default LDAP port used by the LDAP server. The default for Non-SSL requests is 389 and port 636 for SSL.
Use SSL	If the LDAP server you are connecting to is using SSL you must enable this option.

The next section which needs to be configured is the **LDAP Search**. This section defines the location of the sync group and the users which will be synced into the MFT Database. The examples below demonstrate different configurations an Administrator may setup to search for LDAP users (Refer to Figures 2 and 3 as references.)

Example 1: The following example will result in 10 Active Directory users being added to the MFT database (Refer to Figure 2. Users are in orange text boxes):

Figure 6

Example 2: The following example will result in 2 Active Directory users being added to the MFT database (Refer to Figure 2. Accounting Properties window shows 2 users in the Accounting group):

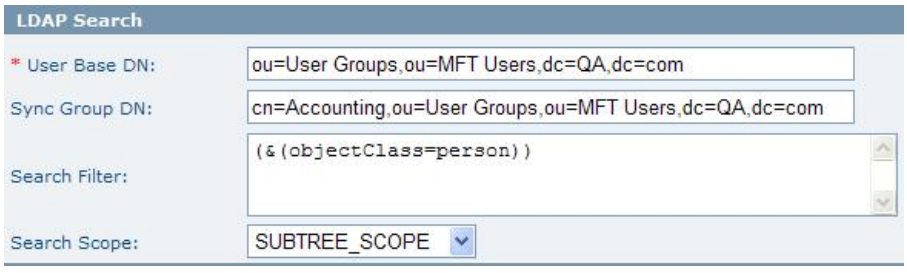


Figure 7

Example 3: If you would prefer to use search filters we can accomplish the same results as in the above example using this setup (Refer to Figure 2. Accounting Properties window shows 2 users in the Accounting group):

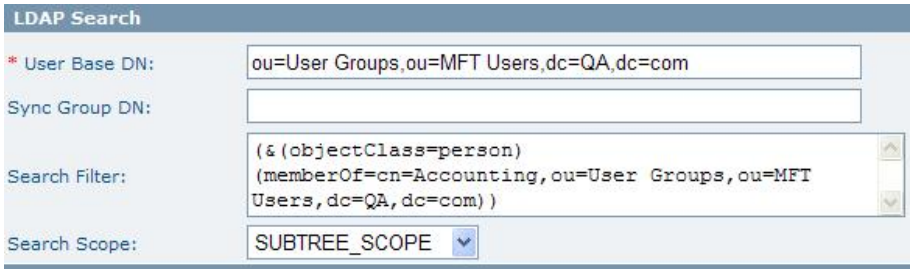


Figure 8

Below are some examples of search filters that could be used when searching for users becomes more detailed:

Filter to sync multiple Security Groups in a single authenticator:
(|(&(objectClass=user)(memberOf=cn=Accounting,ou=User Groups,ou=MFT Users,dc=QA,dc=com))(&(objectClass=user)(memberOf=cn=Finance,ou=User Groups,ou=MFT Users,dc=QA,dc=com)))

Filter to sync all users with mail accounts:
(&(objectclass=user)(mail=*))

Parameter	Definition
User Base DN	The base in the directory tree where users are defined. The levels searched below this base depend on the Search Scope parameter
Sync Group DN	The fully qualified name of the container on the directory server which will be used to associate the users with MFT. Only users who are inside this container will be synchronized with the Database.
Search Filter	The LDAP Search Filter allows you to be more selective of the user objects returned during an LDAP search; it can be used instead of, or in addition to the Sync Group DN. Syncing unnecessary LDAP objects with the MFT Server can be avoided when using an appropriate search filter. For example to sync all users from Active Directory with mail accounts the filter string would be: **(&(objectclass=user)(mail=*))** If you do not wish to use a specified filter to search for users you should change the value to read **(objectClass=user)** Contact your directory server administrator for more details on constructing LDAP Search Filters.
Search Scope	The directory levels below the Base DN that LDAP will search. **SUBTREE_SCOPE** - defines that all levels below the Base DN will be searched. This is the default value and should be used by most users. **ONELEVEL_SCOPE** - defines that only the level defined by the Base DN will be searched. **OBJECT_SCOPE** - defines that only the object defined by the Base DN and the Search Filter will be searched.

The next section is the **LDAP attributes**, these are the fields that LDAP reads from the directory datastore server in order to pull in the correct information. The predefined values in this section should be confirmed with the directory server administrator. In most cases no changes are necessary.

The last section on the Add Authenticator page is **Right Management**. Here you can enable the rights you want to be managed using the LDAP server. MFTCC or MFTIS users can be assigned

various rights which allow them different capabilities. The most popular of these rights is the **TransferRight**; without this right assigned to a user, they cannot perform file transfers. Some LDAP environments may want to control which users are assigned this right and other rights from the LDAP server. Once the right is enabled for management through the LDAP server it cannot be granted or un-granted from MFTCC or MFTIS. A group with the name which is specified on the **LDAP Group Name** field must exist on the directory server and the users granted this right must be members of the group.

The configuration shown here means that any users added from the Active Directory's TransferRight group (Jane Smith and John Doe in the example above) will being given the FileXpress TransferRight when they are added to the database. (Refer to Figure 3. Users are pulled from the TransferRight group):

Figure 9

Parameter	Definition
Right Group Base DN	The location in the directory tree of the OU which contains the MFT Rights
Enable	When the Enable box is checked, that right will be managed on the defined LDAP server.
Right Name	The right as it is recognized by MFT.
LDAP Group Name	The name of the group on the LDAP server which will be associated with the right in MFT, this can be the same as the Right Name or be specified as a different group name. The LDAP Group Name specified in the field should match the group name on the directory server.

Once the configurations have been completed click the **Add** button and the authenticator will be added to the system. You can now run a test to verify your configurations will connect successfully and pull the correct users into the database. To test your configurations navigate to **Administration > Authenticators > Manage Authenticators** (Figure 10 shows our example setup).

1.5.6.2 Manage Authenticators

From the Manage Authenticators panel, authenticators can be updated, deleted, or tested.

To update an Authenticator's configurations, click on the Authenticator Name link to open the Update Authenticator web page. Once the changes are made, click on the Update button to save the changes.

To delete an Authenticator, select the check box next to the Authenticator Name that you wish to delete and click on the Delete button at the bottom of the panel. Multiple Authenticators may be deleted at one time.

To test an Authenticator connection, click on the Test link of the Authenticator Name that you would like to test the connection for. (Figure 10 continues with our example setup):

Figure 10

Click on the Test link to verify connection settings and returned results with MFT Internet Server. Figure 11 below shows 2 users will be synchronized with the MFT Database along with the TransferRight assignment (Refer to Figures 2 through 9 as a reference):

Figure 11

Now that our test was successful it is possible to synchronize users and rights from the directory server through LDAP. If no rights are enabled for the authenticator, the users will be added to the MFT database without any rights when the LDAP sync is performed. It is then the responsibility of the MFT Administrator to assign rights to the users through the MFT Internet Server Administration web pages. The next section describes the process of synchronizing with the LDAP Authenticator.

1.5.7 LDAP Sync

In order to populate the MFT database with LDAP users you would Sync MFT Internet Server with an LDAP server. To bind to the LDAP server you would setup an Authenticator by navigating to the **Administration > Authenticators > Add Authenticator** web page. Refer to the Add Authenticator section for more information. Once the Authenticator is configured and tested you can run an LDAP Sync.

By default, synchronization to the MFT Internet Server database will pull in the directory user's Login Id, Full Name, and Email Address for those contained in the LDAP sync group, as well as any rights assigned to the user if Rights Management is enabled on the authenticator.

To synchronize LDAP Authenticators a user must have the MFTIS **AdministratorRight** assigned to them in the system.

Synchronization is performed three different ways:

1) Manual Sync: A manual sync can be done by the Administrator by going to the LDAP Sync web page to sync a single user or all LDAP users.
2) Scheduled Sync: A scheduled sync can be done once a day by setting up the options found in the LDAP Settings section found by navigating to Administration > System Configurations and expanding the Global Settings box. By default this is disabled. If you have a MFT Command Center and MFT Internet Server sharing the same database the sync can be configured to be performed by either server.
3) Automatic Sync: This sychronixation occurs when an LDAP user logs into the MFTIS system and authenticates against the LDAP server.

Note: If for any reason a user fails to be synchronized, you can find further information on the cause by reading the `ldap_sync_report_messages-MFT-xxxx-xx-xx.txt` report that is located in `<MFT_Install>\logs\message` directory where `xxxx-xx-xx` represents the date the synchronization took place.

1.5.7.1 Manual Sync

In this case, synchronization is manually executed by a Super Administrator. In order to synchronize, log into MFTCC or MFTIS Administration and navigate to: **Administration > LDAP Sync**. This form gives two options for synchronizing. The administrator can sync a single user or all users across all active authenticators. (Figures 12 and 13 demonstrate synchronizing 2 users from our Authenticator configured in Figures 2 through 11.)

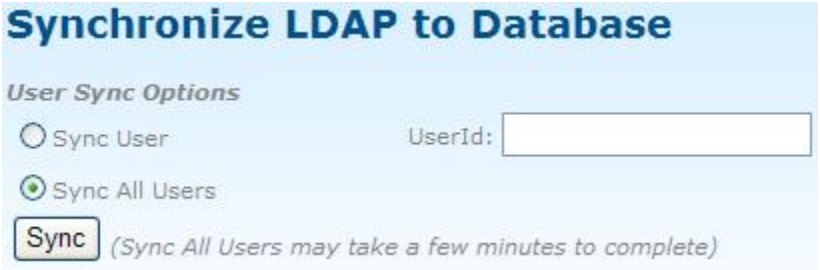


Figure 12

Figure 13

Sync User:
To synchronize a particular user, select the **Sync User** option, type in the user id you wish to sync with in the **UserId** field and then click the **Sync** button.

Sync All Users:
To synchronize all users, select **Sync All Users** and click the **Sync button**. All the users found in the sync groups across all active authenticators will be synchronized with the MFT Database. The total amount of LDAP users and rights (if enabled) synchronized will be displayed at the top of the screen. Note – If an error occurs for one user, the Sync will continue on to the next user.

Once you have synchronized the LDAP users the Administrator can navigate to **Users > Manage Users** web page where they will see the new LDAP users added to the system. Figure 13 below shows our two LDAP users added to the system (Refer to Figures 2 through 12 as references):

Figure 14

Note: When LDAP user ids are synchronized they will be represented in the MFT Database in the format of xxxxx-userid where xxxxx is the Authenticator Name. End users will not need this portion of the userid to login to the system. Example: John Doe (jdoe) would login with jdoe and not AD162-jdoe.

The new users synchronized can now login to MFT using several different userid options. Let's look at John Doe from our example in Figure 14 he can login using the following user ids:

jdoe

QA\jdoe (This is using the LDAP domain)

Note: If an end user has the same LDAP user id in multiple domains that will be synchronized the end user needs to always login with the specific domain\userid they want to connect with.

1.5.7.2 Scheduled Sync

To setup up LDAP Sychronization to be done daily navigate to **Administration > System Configurations** and expanding the Global Settings box. Look for the section labeled LDAP Settings as seen below:

Figure 15

Click on the Sync Server Host Name drop down box. By default this is set to Disabled. Choose the server from the drop down box you want to perform the synchronization to be done by clicking on the name. If you do not have multiple MFT Command Centers or MFT Internet Servers sharing the database you will only see one server listed in the drop down menu.

Next set the Sync Server Start Time.

Click the Update button when you are done to save you configurations.

1.5.7.3 Automatic Sync

An automatic sync occurs every time an LDAP user logs in to the MFT Internet Server system and authenticates against the LDAP server. This ensures any updates to an end users account has come across to the MFT database at the time of login.

1.5.8 Lockout

The MFT user account must have the **AdministratorRight** in order to Release Locks for Users, IP Addresses and the System. When a lock out will occur is configured in the Global Lockout Rules section of the System Configurations web page.

1.5.8.1 Lockout Management

From the Lockout Management web page an Administrator can release a lock that has been placed on a User(s), an IP Address(es), or the System. To release a lock on a single user account, type their MFT user id in the User id field and click on the Release Locks button. If a lock is in place for that user id a message will be displayed the user account has been released. The same will occur if you release a single IP Address. You can release more than one user or IP Address by typing them in separated by a semi colon as seen in out example below:

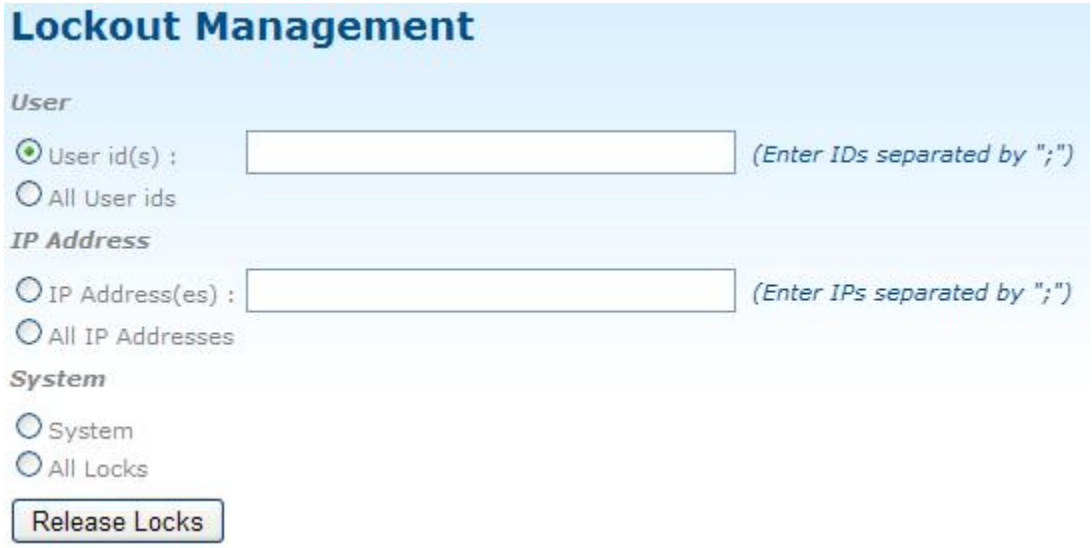
10.97.196.26;10.97.196.101

If all the locks need to be released select either, All User Ids, All IP Addresses, or All Locks and click the Release Locks button.

Note: Validation is not performed on the User Id(s) or IP Addresses entered.

Note: Restarting the webserver will clear all locks.

Navigation: Administration > Lockout > Lockout Management



1.6 Reports

The Reports section contains information for Auditing, Alert History, Diagnostics, Server Statistics and Database Reports.

1.6.1 Audits

The various Audits web pages allow an Administrator to search, delete, and save specific search criteria in a filter for audit records generated by MFT Internet Server audit logs.

1.6.1.1 Search Audits

The Search Audits page allows you to search for completed MFT Internet Server transfers. By default you will see the first 100 audit records for the present day displayed within the Results box. If there are more than 100 audit records, click on "**List Next 100 >**" to access the next 100 audit records.

If you would like to conduct a more detailed search through the audit records expand the Selection Criteria box to display multiple fields that can be used to produce a more detailed search of the audit records contained in the database. You can use a single field or a combination of fields to further define the results you can receive. A percent sign (%) may be used as a wildcard character in all the fields.

To view all the details of an audit record click on the Audit Id to view the complete Audit Details regarding that particular transaction.

The Internet Server transfer records are written and saved in the database when MFT Internet Server transfers are conducted.

Platform Server Manual Poll (Command Center Only:
To run a Platform Server Manual Poll on a remote Platform Server it must have a server definition under Servers in MFT Command Center with a Server Type of Platform Server. This server definition must have the Manage Platform Server selection box enabled under the Management Options expandable configuration box (this is the only option needed to be set at this time for this process). In addition to the server definition being defined you also must have your Collection Service configured and running to collect the audit logs from that Platform Server. Using the Manual Poll search will cause the collector to go out and pull the audit log from the Platform Server in real time and bring it forward for you to view now.

1.6.1.2 Delete Audits

Audit records contained in the database can be deleted when necessary. To delete audit records an MFT Internet Server user can have either the **AdministratorRight** or **DeleteAuditRight** in order to delete audit records.

To delete audit records, select a Date or Number of Days as well as the Audit Type, and then click on the Delete button at the bottom of the panel.

1.6.1.3 Audit Search Filters

While an Administrator can use the Search Audits web page Selection Criteria box to define exactly what audits he wants to view they would have to do this every time they went to the Search Audit web page. The Audit Search Filters allows an Administrator to define the search criteria he wants and then save it to be used over and over again.

To add or manage audit search filters the user must have either the **AdministratorRight** assigned to them. Please refer to the on line Help screen for detailed descriptions for each field available to be configured on the Add Audit Search Filter and Manage Audit Search Filters web pages.

1.6.1.3.1 Add Audit Search Filter

The Add Audit Search Filter page allows you to pre-define the selection criteria used to display MFT Internet Server and Platform Server audit records. The Audit Search Filter Selection Criteria box allows you to define filters to limit the number of audit records that will be displayed. Once the Selection Criteria is complete, press **Add** to Add the entry to the Audit Search Filter. To execute an Audit Filter, navigate to the **Reports > Audits > Search Audits** web page and select the filter from the **Retrieve pre-selected filter** drop down box within the Selection Criteria box.

1.6.1.3.2 Manage Audit Search Filter

When you need to update a Audit Search Filter you have saved in the system you would go to the Manage Audit Search Filters web page. This page will list the first 100 defined Audit Search Filters saved in the database. If there are more than 100 Audit Filters click on "**List Next 100 >**" to access the next 100 audit filter definitions. Use the Back button to see the previous definitions.

To update an Audit Filter definition, click on the Search Audit Id of the definition that you would like to change. Make the necessary changes and click the Update button.

To delete an Audit Filter definition, click on the empty box under the Delete column next to the Search Audit Id that you wish to delete in order to select it for deletion then click the Delete button at the bottom of the panel. Multiple Audit Filters may be deleted at one time.

1.6.2 Diagnostics

The Diagnostics page displays information that assists TIBCO Technical Support in solving issues with the Command Center and Internet Server. Note that on the left side of the page, under the heading “Diagnostics” is the link **Save to File.** This allows you to save the page image to a file. By clicking on **Save to File** the Browser download page will be displayed asking whether you want to Open the file or Save it to disk. Select Save to Disk to save the file to disk. The exact page format and the location of the file are dependent on the WEB browser that you are using.

The Diagnostics page is broken up into the following sections:

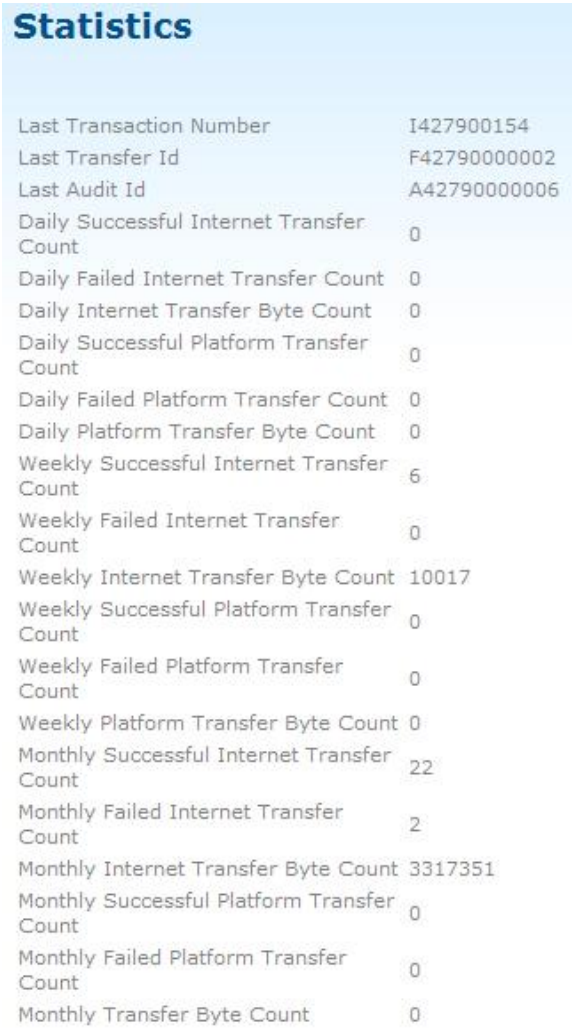
Version Information	Shows information about the Internet Server Version and Build, as well as the J2EE server type and version.
Install Paths	Shows the path where the Internet Server was installed.
Database Info	Shows how many connections to the database are present.
License Keys	Shows the License Key information.
JVM Settings	Shows the details for the J Virtual Machine Memory.
JVM System Properties	Displays information about the JAVA Virtual Machine.
Web.xml Context Parameters	Contains information located in the Web.xml file.
File Information	Shows the path and date/time of files located in the MFT Internet Server/Internet Server Context (cfcc) as well as important JAVA files.

1.6.3 Statistics

Navigation:

Reports > Statistics

The Statistics web page displays daily, weekly and monthly transfer byte counts and more. Below is a list of the various statistics available:



Statistics

Last Transaction Number	I427900154
Last Transfer Id	F42790000002
Last Audit Id	A42790000006
Daily Successful Internet Transfer Count	0
Daily Failed Internet Transfer Count	0
Daily Internet Transfer Byte Count	0
Daily Successful Platform Transfer Count	0
Daily Failed Platform Transfer Count	0
Daily Platform Transfer Byte Count	0
Weekly Successful Internet Transfer Count	6
Weekly Failed Internet Transfer Count	0
Weekly Internet Transfer Byte Count	10017
Weekly Successful Platform Transfer Count	0
Weekly Failed Platform Transfer Count	0
Weekly Platform Transfer Byte Count	0
Monthly Successful Internet Transfer Count	22
Monthly Failed Internet Transfer Count	2
Monthly Internet Transfer Byte Count	3317351
Monthly Successful Platform Transfer Count	0
Monthly Failed Platform Transfer Count	0
Monthly Transfer Byte Count	0

1.7 ***Help***

Eachweb page displays a Help icon, 

. Click on the icon to display more detail information regarding the web page and the fields provided.

2

2 Delegated Administration

Delegated Administration offers a MFT Internet Server administrator the ability to divide the system into smaller units which can be managed independently of one another. This sub division of the system offers greater security and eases of burden of administration on a single administrator. It allows businesses to create a system based on their organizational structure. Internal divisions of a corporation and external partners can be given autonomous control over the management of their users and transfers.

These smaller units, called Departments, can have one or more administrators assigned to manage them. The Department Administrator's domain is over the Users, Groups, Transfers, Servers and Audit records assigned to the Department. They cannot administer anything else in the system. The existing system rights, such as UpdateTransferDefinitionRight, can also be applied to a Department Administrator thus offering a finer granularity of administrative control.

Administrators who are not assigned to a Department are considered "Super" Administrators who can manage the entire system. While Department Administrators can only manage one Department, Super Administrators have access to all Departments in the system. They are the only ones who can administer License Keys, Servers, System Configuration, FTP server configuration and Checkpoints. They are also the only ones who can add Departments and change the Department to which a User, Group, Transfer or Server is assigned.

An administrator can further limit the access to his Users, Groups and Servers through the use of "Visibility". This "Visibility" allows Departments to interact with each other without giving up administrative control. When applied to Users, Groups and Servers, Visibility allows Departments to expose or hide these items from each other. This is achieved by setting the Visibility to public or private. For example, the Sales Department can create a transfer and give authorization for that transfer to a "public" user in the Accounting Department. The administrative control of the transfer still belongs to the Sales Department that created it but the ability to transfer the file is given to a user in the Accounting Department. The Sales Department can in no way alter the attributes of the user from the Accounting Department. If this Accounting User had been "private", the Sales Department could not give him authorization to transfer the file. In this case the user is effectively "hidden" from other Departments.

This design allows existing customers to keep their system as it is and gives new customers the option not to use these features. In these cases all administrators are Super Administrators and Transfer Users, Groups, Servers and Audit records are not assigned to any Department. The system functions with respect to administration as it did in versions prior to version 2.2 of SIFT.

2.1 Administrative Functions and Rules

This section will list the tasks that administrators can perform and how Departments and Visibility affect those tasks. The tasks are grouped by administrative item. A description is given of what the task does when performed by a Department Administrator and what it does when performed by a Super Administrator.

2.1.1 Active Users

A user with UpdateSessionRight can delete and view active users. A user with ViewSessionRight can only view active users.

Department Administrator	A Department Administrator with ViewSessionRight can only view active users in their department. A Department Administrator with UpdateSessionRight can delete and view active users in their department.
Super Administrator	Can view or delete any active user.

2.1.2 Audits

Audits records will be assigned to the department from which the corresponding transfer definition is assigned. Audit records do not have a visibility associated with them. An audit record can only belong to one department in the system. A Department Administrator can only view the audit records assigned to his department. The exception to this rule occurs when the Department Administrator does searches on audit records. Please reference the "Search Audit" section below for details. A user with ViewAuditRight can perform audit searches.

2.1.2.1 Search Audits

Department Administrator	Searches for and displays audit records that have been assigned to this administrator's department. When performing a search based on User ID, Group ID or Server name only those that have been assigned to this department can be used as search criteria. The Department Administrator will only be able to view the audit records of file transfers assigned to his department, except in the case when a search is done based on a specific Transfer User Id or a specific Audit ID. Doing a search on a specific Transfer User ID will return all audit records for that User no matter which department the transfer is assigned to. In the same way, doing a search on a specific Audit ID will return the audit record for the transfer no matter which department the transfer is assigned to. This extended search capability is provided as a convenience for Department Administrators.
Super Administrator	Searches for and displays all audit records in the system.

2.1.2.2 Delete Audits

Department Administrator	Cannot delete any audit records in the system with only the AdministratorRight. This can only be performed if the DeleteAuditRight is given. In this case, department checking will not be done.
Super Administrator	Delete any audit record in the system.

2.1.3 Departments

The department administrative tasks can only be performed by a Super Administrator. The Department Administrator can only manage the users assigned to his own department.

2.1.3.1 Add Department

Department Administrator	Cannot perform this task.
Super Administrator	Adds a Department to the system.

2.1.3.2 Manage Department

Department Administrator	Cannot perform this task.
Super Administrator	Can list, update and delete all Departments in the system.

2.1.4 Diagnostics

Only a Super Administrator can perform this task.

2.1.5 FTP Server Configuration

Only a Super Administrator can perform these tasks.

2.1.6 Groups

Groups can be assigned to a specific department and they can have a public or private visibility.

Granting a group private visibility means that public Users from all departments and the private users from its own department can be added to it, but this Group ID will not be seen by the administrators from other departments. This group can be set as the Authorized Group Id in a File Transfer definition that is assigned to this department. This group can also be used as the Group ID value in a User Profile definition for public and private Nodes in this specific department.

Granting a group public visibility means that this group can do what a private group can do plus this Group ID will be seen and available to all Department Administrators in the system. This group can have public Users from other departments added to it, and the group can be set as the Authorized Group Id in a File Transfer definition that is assigned to other departments. The group can be used as the Group ID parameter value in a User Profile definition created for public Nodes assigned to other departments. Group IDs must be unique throughout the system, thus Groups in different departments cannot have the same Group ID. A group can only belong to one department in the system.

A Department Administrator can see Groups assigned to his Department as well as Groups from other Departments that have a Visibility of public. If a Super Administrator updates a Group originally created by the Department Administrator, then only the information that the Department Administrator has access to can be used. Otherwise, an error will occur.

UpdateGroupRight enables a user to add, update, delete and view Groups. ViewGroupRight enables a user to view Groups.

2.1.6.1 Add Group

Department Administrator	Creates a group, which is assigned to this administrator's department. The group's visibility can be set to public or private.
Super Administrator	Creates a group whose department can be set to any department in the system or to none at all. The group's visibility can be set to public or private. A group that is not assigned to a department gains no special properties but can only be administered by a Super Administrator.

2.1.6.2 Manage Groups

Department Administrator	Can update and delete any Groups that have been assigned to this administrator's Department. The Department Administrator cannot see or change the Department parameter that a Group has been initially assigned to. Only the Super Administrator can do this. The Visibility of the Group can be changed to public or private by the Department Administrator.
Super Administrator	Can list, update and delete any Group in the system. The Department that this Group has been assigned to can be changed to any Department in the system or to none at all. The Visibility of the Group can be changed to public or private. Care should be taken when changing the Visibility of a Group since it may include or exclude Users when this change is made.

2.1.7 Internet Checkpoints

Only a Super Administrator can perform this task.

2.1.8 Internet Transfers

Internet Transfers can be assigned to Departments. A transfer can be assigned to only one Department in the system. The administrator can choose not to assign a Department to the transfer, but this offers no special properties to the transfer. If a Transfer has not been assigned to a particular Department, then it can only be administered by a Super Administrator. Transfers do not have a Visibility associated with them. Department Administrators cannot access or view another Department's transfers. When a User with Transfer Rights logs in to perform a transfer, they will see all the transfers that they are authorized to access, regardless of the Departments to which the transfers have been assigned.

A Department Administrator can see Users, Groups and Servers assigned to his Department as well as Users, Groups and Servers from other Departments that have a Visibility of public. If a Super Administrator updates a Transfer definition originally created by the Department Administrator, then only the information that the Department Administrator has access to can be used. Otherwise, an error will occur. Only the Super Administrator can change the Department that a Transfer has been assigned to. Care should be taken when changing the Department on a Transfer definition. The User and Group Visibility need to be considered.

UpdateTransferDefinitionRight enables a user to add, update, delete and view Internet Transfers.
ViewTransferDefinitionRight enables a user to view an Internet Transfer definition.

2.1.8.1 Add Internet Transfer

Department Administrator	Creates a transfer that is assigned to this administrator's department. When selecting the Authorized User Id, Group Id, or server only users assigned to the same department can be used, as well as users, groups, or servers from other departments with public visibility.
Super Administrator	Creates a file whose Department can be set to any Department in the system or set to blank. When selecting the Authorized User Id, Group Id, or Server it can be any user, group, or server assigned to the Department chosen or any public user, group or server from another Department in the system.

2.1.8.2 Add From Existing Transfer

Department Administrator	Creates a new transfer that is assigned to the administrator's department. The new transfer can only be created from a pre-existing transfer from the same department. When selecting the Authorized User Id, Authorized Group Id, or Server Name, only users, groups, or servers which are assigned to this department; as well as users, groups, or servers from other departments with public visibility can be used.
Super Administrator	Creates a transfer whose Department can be set to any Department in the system or set to blank. The new transfer definition can only be created from a pre-existing transfer definition. When selecting the Authorized User Id, Authorized Group Id or Server Name it can be any user, group, or server assigned to the chosen Department or any public user, group, or server from another Department.

2.1.8.3 Manage Transfers

Department Administrator	Can list, update and delete Internet Transfers that are assigned to the administrator's department. When selecting the Authorized User Id, Authorized Group ID, or Server only the users, group, or servers assigned to the same department can be used; as well as users, groups, or servers from other departments with public visibility. The department parameter cannot be changed and therefore will not be displayed on the Update Transfer page. Only the Super

	Administrator can change the department a transfer has been assigned to.
Super Administrator	Can list, update and delete any Internet Transfer Definition in the system. When updating the Authorized User Id, Group Id, or Server parameter, only Users ID's, Group Ids, or Servers assigned to the Department that owns the Transfer or Users, Groups, or Servers from other Departments with public Visibility can be used as the new value. Please keep in mind that a Super Administrator will see all information in the pull-down menus, but he must comply with the rules stated above for the Department Administrator or an error will occur. Only the Super Administrator can change the Department that a file has been assigned to. Care should be taken when changing the Department on a Transfer definition. The User and Group Visibility need to be considered.

2.1.9 License

The Department Administrator cannot administer license keys. The Super Administrator will be the only one who can perform this task.

2.1.10 Server

Servers can be assigned to Departments and they can have a public or private Visibility. The Super Administrator will be the only one who can perform the tasks of creating and configuring Servers and assigning them to the particular Departments. The Department Administrator cannot administer Servers, but can list all Servers assigned to his Department and public Servers assigned to other Departments. Assigning private Visibility to a Server means that it can be set as the Server for a file transfer for a particular Department. The Servers can be associated with this Server for public and private Users or Groups in this Department. Assigning public Visibility to a Server means that in addition to the features granted by private Visibility the Server can also be set as the Server Name value in a file transfer assigned to another Department. Public Visibility also means that a Server can be associated with this Server for public Users and Groups belonging to another Department. A Server can only belong to one Department in the system. The administrator can choose not to assign the Server to a Department, but this offers no special properties to the Server.

UpdateServerRight enables a user to add, update, delete and view Servers. ViewServerRight enables a user to view a Server.

2.1.10.1 Add Server

Department Administrator	Cannot perform this task
Super Administrator	Creates a Server whose Department can be set to any Department in the system or set to none. A Server that is not assigned to a Department has no special properties.

2.1.10.2 Update Server

Department Administrator	Cannot perform this task
Super Administrator	Can update and delete all Servers in the system. The Department that the Server has been assigned to can be changed to any Department in the system or to none.

2.1.11 Server Credentials

Administrative tasks associated with Severs Credentials can be limited by the Rights that are assigned (or not assigned) to a user. The Department Administrator cannot administer Server Credentials unless they are given UpdateServerCredentialRight. Otherwise, the Super Administrator will be the only one who can perform these tasks. Users and Groups associated with Server Credentials can only be mapped to Servers that are assigned to their Departments or public Servers in other Departments. A private User or Group in a Department can never be mapped to a Server that is not assigned to that User or Group's Department.

ViewServerCredentialRight enables a user to view Credentials.

2.1.11.1 Add Server Credentials

Department Administrator	Cannot perform this task unless specifically given UpdateServerCredentialRight.
Super Administrator	Adds a Server Credential to the system. Users and Groups can only be mapped to Nodes that are assigned to their Departments or public Nodes in other Departments.

2.1.11.2 Manage Server Credential Credentials

Department Administrator	Can list, update and delete Server Credentials if they are given the proper Rights. In addition to AdministratorRight, administrative users must also be given UpdateServerCredentialRight in order to perform this function.
Super Administrator	Can list, update and delete any Server Credential definition in the system.

2.1.12 Statistics

Only a Super Administrator can perform this task.

2.1.13 System Configuration

Only a Super Administrator can perform these tasks.

2.1.14 Users

Users can be assigned to Departments and they can have a public or private Visibility. Granting a user private Visibility means he can be added to public and private Groups that have been assigned to his Department, he can be set as the authorized user of Transfer definitions that have been assigned to his Department and he can have a Server Credential created for public and private Servers assigned to his Department. Granting a user public Visibility means he can do what a private user can do and can be added to a public Group assigned to another Department, set as the authorized user of a Transfer definition that is assigned to another Department and he can also have a Server Credential created for a public Server assigned to another Department. User ids must be unique throughout the system, thus users in different Departments cannot have the same user id. A user can belong to only one Department in the system.

UpdateTransferUserRight enables a user to update users who have only TransferRight. ViewUserRight enables a user to view users.

2.1.14.1 Add User

Department Administrator	Can create Users with TransferRight (default) who are automatically assigned to the administrator's Department. The Department Administrator can also create Users who are assigned to the administrator's Department and who can have any one of the system administrative rights within the Department. This means a Department Administrator cannot create a Super Administrator, but he can create another administrator for his Department. The User's Visibility can be set to public or private. Setting Visibility to public will make this User visible and available for all other Department Administrators in the system.
Super Administrator	Same as the Department Administrator but the User can be assigned to any Department in the system or to none at all. A Super Administrator can create Super Administrators and Department Administrators, as well as Users with any available rights. If a User is not assigned to a Department the User gains no special properties. This means that the User can only be administered by a Super Administrator.

2.1.14.2 Add From Existing User

Department Administrator	Using this feature the Department Administrator can create a new User who is automatically assigned to this administrator's Department. The new User can be created only from a pre-existing User from this Department. The new User will automatically be given Rights depending on the User that is being used as a template. However, a Department Administrator cannot give the new user any Rights that he does not have. For example, a Department Administrator who only has AdministratorRight cannot assign UpdateServerCredentialRight to a new user.
Super Administrator	Using this feature, the Super Administrator can create a User who can be assigned to any Department in the system or to no Department at all. The new user can only be created from any pre-existing user in the system and will be given all the Rights that the existing user possesses.

2.1.14.3 Manage User

Department Administrator	Can update Users who have been assigned to this administrator's Department. The Department that the user has been assigned to cannot be changed to another Department by this Department Administrator. Only the Super Administrator can assign the User to another Department. Visibility of the user can be changed to public or private by the Department Administrator
Super Administrator	Can list, update and delete all Users in the system. The Department that the User has been assigned to can be changed to any Department in the system or to none at all. Visibility of the user can be changed to public or private.

3

3 Extended Features

MFT Internet Server has several extended features such as directory transfers, email notification, file token substitution, multiple language support, LDAP support, FTP and SSH support, and using the Administrator and Internet Server Command Line Utilities.

Note: This section does not go into detail about how to run the Administrator or Internet Server Command Line Utility locally. It only goes into detail about how to execute the Administrator Command Line Utility via an MFT Platform Server transfer request. Likewise, this section does not go into detail about how to install and configure the Administrator Command Line Utility. See the *Command Line Utilities Guide* for more information about configuring the Administrator Command Line Utility.

3.1 Internet Server Command Line Utility

3.1.1 Executing Internet Server File Transfer as a Post Processing Action

The Add Transfer section of this manual contains a section called Post Processing Actions (PPA). These will allow you to perform up to four actions to be completed by the responding Server when a file transfer request has completed. You can use this function to execute an MFT Internet Server Command Line Client command as a Post Processing Action (PPA). Note: For more information about the Internet Server Command Line Utility please see the MFT Internet Server Command Line Utilities Guide. The advantage of doing this is that you can perform a file transfer and then execute for instance, a file transfer command line utility command within a single step.

1. The Internet Server Command Line Client Utility must be installed and configured on the system(s) where the file transfer runs.

When using PPA to initiate an MFT Internet Server Command Line Utility command or any command for that matter, it is a good idea to get the command running successfully in batch mode first. For this example first use the file transfer command for the Internet Server Command Line Client Utility to ensure

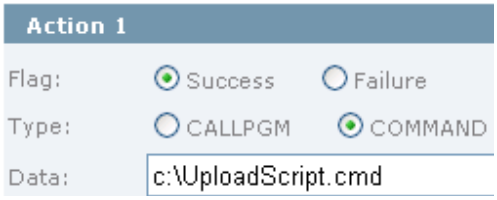
that the request executes successfully. Once the command is running successfully you can add it as a PPA request.

For this example, let's say you want to upload a file to the Internet Server. Once that file transfer request completes you want to launch a script that uses the command line utility to send that file to another MFT server.

You would first make sure your Internet Server command ran successfully from a batch job by testing it out. Here is an example (File name is **UploadScript.cmd**):

cd InternetCommandLine
call setutilcp
java cfcc.CFInternet a:ProcessFile Description:UploadToAIX

Now I will add my script to a Post Processing Action in my MFT Internet Server transfer definition:



Now each time this transfer request is run this PPA will start upon the success of the file transferring successfully.

3.1.2 Configuring the target MFT Internet Server system

MFT Internet Server comes with a script that will work when a user issues Aministrator Command Line Utility commands. When you want to execute the Aministrator Command Line Utility command as part of a file transfer request, then you must create a new script that is tailored for the environment that you are running. The next sections show how the scripts can be generated for the Windows and UNIX environments.

3.1.3 Configuring Windows environment

When the Administrator Command Line Utility client (CFAdmin) is installed on a Windows computer, a file called cfcc.bat is created. The example shown below uses a copy of the cfcc.bat file called cfccmf.bat. It is the base program with some additional parameters set in it.

```
e:
cd cfcc\MFTAdminCL
set PATH=%PATH%;c:\program files\java\j2re1.4.2_04\bin; ;
call setutilcp
java cfcc.CFAdmin t:%1.xml %2 %3 %4 %5 %6 %7 %8 %9
```

The above script performs the following functions:

1. It sets the drive to the drive where the cfccmf.bat file is located. In this case, the cfccmf.bat file is located on the E: drive.
2. It sets the directory to the directory where the cfccmf.bat file is located. In this case, the cfccmf.bat file is located in the cfcc\MFTAdminCL directory.
3. It sets the PATH to include the Java JRE (Java Runtime Environment). If the correct JRE is already included in the PATH, then this step can be skipped.
4. It calls the setutilcp.bat file included with the Aministrator Command Line Utility. This file sets up environment variables needed by Java to execute.
5. The last statement is the actual Java command that executes the Aministrator Command Line Utility. Note that the Aministrator Command Line Utility is named CFAdmin. Note that even on Windows, the Java program name (CFAdmin) is case sensitive. The first parameter (t:%1.xml) shows that the

first parameter entered should be the name of the XML template file without the .xml suffix. Parameters %2 through %9 give you the ability to override up to 8 parameters defined in the template XML file.

3.1.4 Configuring UNIX environment

When the CFAdmin client is installed on a UNIX computer, a file called cfcc.sh is created. The example shown below uses a copy of the cfcc.sh file called cfccmf.sh. It is the base program with some additional parameters set in it.

```
#!/usr/bin/ksh
cd /cfcc
# Set the PATH to include the Java JRE
export PATH=./:/usr/AppServer/java/bin:$PATH
# Set the Java environment variables (copied from setutilcp.sh)
export CLASSPATH=.:ClientCommon.jar:axis-ant.jar:axis.jar:commons-discovery.jar:commons-
logging.jar:jaxrpc.jar:log4j-1.2.4.ja
r:saaj.jar:wsdl4j.jar:trace.jar:CFAdmin.jar:jcert.jar:jnet.jar:jsse.jar:xalan.jar:xercesImpl.jar:
xmlParserAPIs.jar
# Execute the Java CFAdmin
java cfcc.CFAdmin t:$1.xml $2 $3 $4 $5 $6 $7 $8 $9
```

The above script performs the following functions:

1. The first line (#!/usr/bin/ksh) is required and tells the UNIX system to use the korn shell to execute this procedure.
2. It then sets the directory to the directory where the cfccmf.sh file is located. In this case, the cfccmf.sh file is located in the /cfcc directory.
3. The export PATH statement updates the PATH to include the JRE (Java Runtime Environment) executables. If the default PATH includes this directory then this step is not needed.
4. The export CLASSPATH statement was copied from the setutilcp.sh script. This sets up the Java environment variables. Although it looks like four lines of data, it is actually one long statement.
5. The last statement is the actual Java command that executes the Administrator Command Line Utility. Note that the Administrator Command Line Utility is named CFAdmin. The Java program name (CFAdmin) is case sensitive. The first parameter (t:%1.xml) shows that the first parameter entered should be the name of the XML template file without the .xml suffix. Parameters %2 through %9 give you the ability to override up to 8 parameters defined in the template XML file.

3.1.5 Template Users

The following users are automatically added as “template” users to the database during the MFT Internet Server installation process. Other users can then be added based on these templates by using the **Add From Existing User** link. Any Rights assigned to a template user will also be copied to a new user.

User ID	Rights Assigned
admin	AdministratorRight TransferRight
HelpDeskUser	HelpDeskRight UpdateSessionRight ViewAlertRight ViewAuditRight ViewUserRight
TransferUser	TransferRight
AuditorUser	ViewAlertRight ViewAuditRight ViewGroupRight ViewServerCredentialRight ViewServerRight ViewTransferDefinitionRight ViewUserRight

A Collector Id is also added by default. This id is used to create a Server Credential for a Server that will also have the collection option turned on. There are no rights given to the Collector id.

3.1.6 Applet Wrapper

3.1.6.1 Prerequisite

Before you can use the applet wrapper to transfer a file, users should understand the following concept and working flow used by MFT Internet Server. Any concepts not explained here should be defined in other part of the manual.

Note: The definitions/explanations given here might be different that those defined in other parts of this documentation. The definitions/explanations here are for developers to understand the internal working flow of MFT Internet Server for transferring a file so that they can use MFT Command Center SOAP calls to get the necessary information about a file, then use this applet wrapper to transfer a file.

File Record
A file record is a record in the MFT Internet Server database that represents a file. You can view all properties of a file using the web interface or the command line utility (file transfer utility reveals less information than the admin utility). The important properties for file transfer are:

- **FileId**
  The File id property must be used to set 'fileID' value of the applet wrapper.
- **SendRecvFlag**
  This is a flag which indicates the transfer direction. The 'transferDirection' of the applet wrapper must be set according to this value. 'S' – 'SEND'; 'R' – 'RECEIVE'.
- **CompressType**
  This is a flag which is used to indicate if the transfer is compressed. The 'compression' of the applet wrapper must be set according to this value. '0' – 'NO'; '1' – 'YES'.
- **ChkptRestartFlag**
  This is a flag which indicates if checkpoint restart is turned on for the transfer. The 'restartTransfer' of the applet wrapper must be set according to this value. '0' – 'NO', '1' – 'YES'.
- **ChkptInterval**
  This property specifies the checkpoint interval in seconds. The 'checkpointInterval' of the applet wrapper must be set according to this value. The value in file record is minutes. If set per that value, must convert minutes to seconds by multiplying by 60.
- **DirectoryTransfer**
  A flag to indicate if the transfer is a directory transfer. '1' is directory transfer; '0' is not. The applet wrapper acts differently for a directory transfer. The following sections contain more details on directory transfers.

Directory Transfer
MFT Internet Server can transfer a whole directory to or from the server. Inside the implementation, MFT Internet Server can transfer one file at a time to fulfill the directory transfer.

Before any file transfer, the user must know if the transfer if a file transfer or a directory transfer by selecting 'DirectoryTransfer' in the file record. If it is a file transfer, just set necessary parameters of the applet wrapper (see the section of Class Parameters) and do the transfer. If it is a directory transfer, it is divided into two (2) situations:

- **Directory upload**
  Set the 'localFileName' of the applet wrapper and transfer each file in the directory same as a normal file transfer.
- **Directory download**
  Set the 'serverFileName' of the applet wrapper and download each file in the server's directory. The server file name is file name specified by the server for each file under its directory.

3.1.6.2 Get Directory File List

To get server file names for directory download, in file record for directory download, the method 'getDirectoryFileList()' of the file record will return FTClient.DirectoryElementList[], an array of FTClient.DirectoryElementList, which will represent the structure of the directory to be downloaded. The user should parse the structure to get the entire list of server file names.

Structure of FTClient.DirectoryElementList
Major part of source code of this class (extracted from FTClient.jar file) is listed below:

```
package FTClient;

public class DirectoryElementList  implements java.io.Serializable {
    private java.lang.String elementName;
    private java.lang.String elementType;
    private FTClient.DirectoryElementList[] subDirectoryList;

    public DirectoryElementList() {
    }

    public java.lang.String getElementName() {
        return elementName;
    }

    public void setElementName(java.lang.String elementName) {
        this.elementName = elementName;
    }

    public java.lang.String getElementType() {
        return elementType;
    }

    public void setElementType(java.lang.String elementType) {
        this.elementType = elementType;
    }

    public FTClient.DirectoryElementList[] getSubDirectoryList() {
        return subDirectoryList;
    }

    public void setSubDirectoryList(FTClient.DirectoryElementList[] subDirectoryList) {
        this.subDirectoryList = subDirectoryList;
   }

   …
}
```

If the elementType of 'F', it is the leaf node, the elementName is one server file name. If the elementType is 'D', then, it is a sub directory, users should go into the directory, maybe recursively, to find file name.

3.1.6.3 How to Use The Applet Wrapper

MFT Internet Server uses a Java applet to transfer files. For ease of use, MFT Internet Server provides a wrapper class, SIFTSingleFileTransfer, to wrap the details of how to use the applet. Users can create an instance of the class, set necessary parameters and then transfer a file. The class makes one file transfer at a time.

Users need to exam the file record - for example, via soap calls - to get necessary information about a file in order to set some parameters of the applet wrapper.

Class Parameters
Before transferring a file, the following parameters must be set using set methods:

- "fileTransferServletURL" - URL used to contact the file transfer servlet, for example, https://server:port/cfcc/control?view=servlet/fileTransfer
  The user must set this parameter before doing a transfer.

- "transferDirection" - this parameter should be set to "SEND" if the applet is sending and "RECEIVE" if the applet is receiving. Default is “RECEIVE”.
  This value must be set based on the value in the file record.
- "fileID" - file ID representing the transfer record to be transferred.
  This value must be the same as what is in the file record.
- "localFileName" - path and name of local file to be transferred.
  The user must set this value.
- "serverFileName" - Name of server file to be downloaded for a directory transfer. Only to be used when receiving a file from a directory file record.
  Must set this parameter for directory download.
- "sessionID" - id of the current session.
  Must set this id. Got the value from previous SOAP call of getSession().
- "compression" - "YES" if compression is used, "NO" if it is not. Default is “YES”. Must set this value based on the value in the file record.
- "traceLevel" - level of trace to use. This parameter is optional.
- "user id" - User id to be used in an HTTP request requiring BASIC authentication. This is a required parameter.
- "password" - Password to be used in an HTTP request requiring BASIC authentication. This is a required parameter.
- "restartTransfer" - "YES" if transfer is to be restarted, else "NO". Default is “NO”. This parameter is optional. If set, must be based on the value in the file record.
- "checkpointInterval" - Number of seconds between checkpoints.
  This is a required parameter if ‘restartTransfer’ is set.
- "synchronize" - "YES" if multiple instantiated applets are to wait to perform transfer one at a time, "NO" if all applets are to perform the transfer at the earliest chance. Default is “YES”. This parameter is optional.

After set necessary parameters, call transferSingleFile() method to transfer the file.

Get Result
The class provides following information for the transfer:

- "returnCode" - return code from applet
- "bytesTransfered" - bytes transferred
- "compressedByte" - compressed bytes transferred
- "returnMsg" - return message from server

Classpath
The SIFTSingleFileTransfer class is in NonGUIApplet_0.0.0.1.jar file, which will be in the directory after installing Internet command line utility. Put the NonGUIApplet_0.0.0.1.jar file in your classpath when compiling and running your application.

3.1.6.3.1Example 1: Upload a file to server

```
…
import com.tibco.cfcc.fileTransferApplet.nongui.*;
…
//create an instance and set parameters
SIFTSingleFileTransfer xfr = new SIFTSingleFileTransfer();
xfr.setFileTransferServletURL(“location of file transfer servlet”);
xfr.setTransferDirection(“SEND”); // it is an upload file per file record
xfr.setFileID(“file id”);         // the file id in the file record
xfr.setSessionID(“session id”);           // the current session id from server
xfr.setCompression(“YES or NO”);  // depending value in file record
xfr.setUser id(“user who initiates the transfer”);
xfr.setPassword(“user’s password”);

//transfer the file
xfr. transferSingleFile();

//get result
int rc=xfr.getReturnCode();
```



```
long bytes=xfr.getBytesTransfered();
long cbytes=xfr.getCompressedByte();
String msg=xfr.getReturnMsg();
```

3.1.6.3.2Example 2: Download one file from server's directory

```
…
import com.tibco.cfcc.fileTransferApplet.nongui.*;
…
//create an instance and set parameters
… same as example 1, except
xfr.setTransferDirection("RECEIVE");              // it is a download file per file record
xfr.setServerFileName("file name to be downloaded"); //only for directory download

//transfer the file
… same as example 1

//get result
… same as example 1
```

3.2 ***Directory Transfers***

MFT Internet Server has the ability to transfer directories and subdirectories using one Transfer definition. This section will describe how to use the directory transfer definition in the web pages as well as in the Internet Transfer command line. Please be careful when defining directory transfers due to the way that uploads and downloads are handled vary.

When adding a Transfer definition, there is a parameter called "Directory Transfer". This radio button should be chosen if you wish to define a directory transfer. File tokens can be used, but only in the Server File Name (and only for Uploads). Please refer to the "Add File" section of this document for details on adding an Internet Transfer definition to MFT Internet Server.

3.2.1 Directory Transfers using the Thin Client

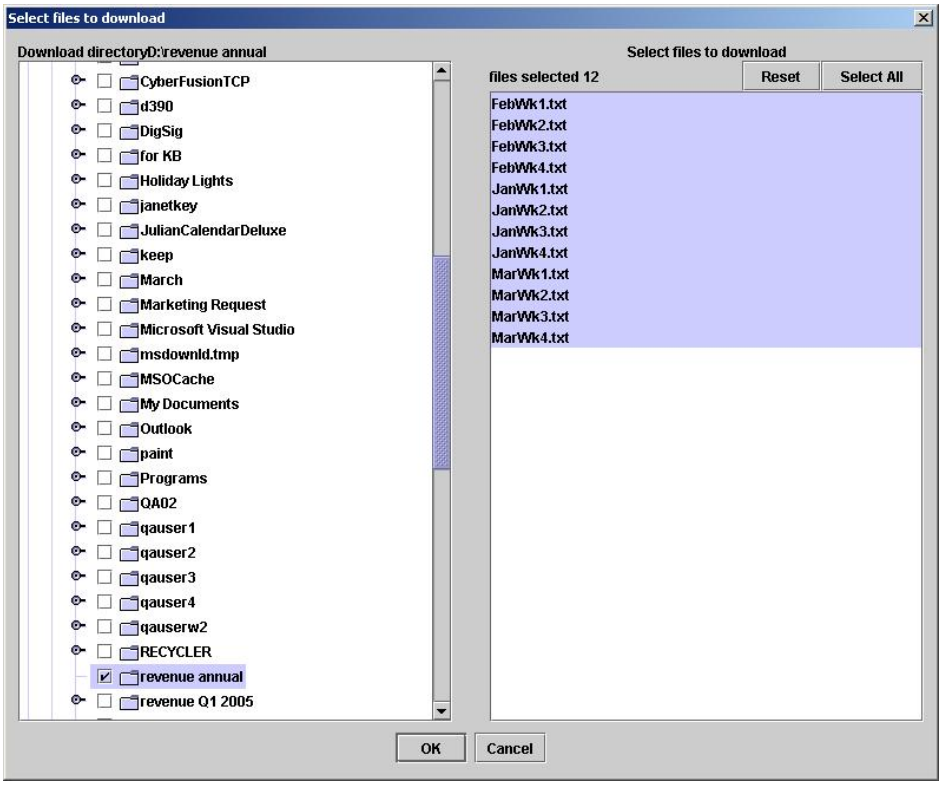
To do a directory transfer, the user would sign on to MFT Internet Server. This will bring the user directly into the Transfers page. The following page will be displayed. This is the same page that is displayed for a file transfer.

A red Browse folder icon indicates a directory transfer. A white Browse file icon indicates that this is a single file transfer.

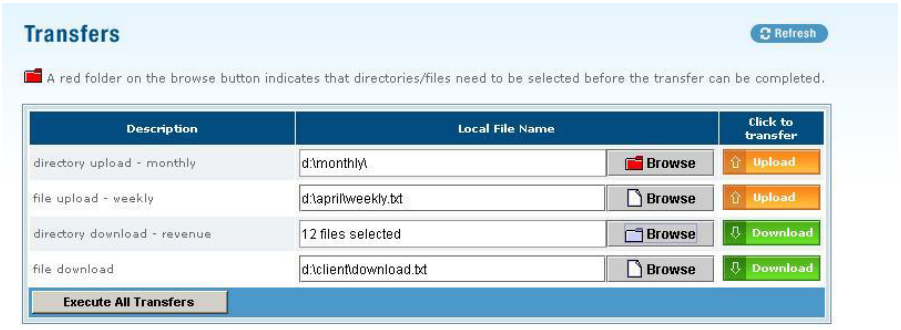
3.2.1.1 Directory Download

In order to download a directory, click the Browse button displaying a red folder icon next to the Local File Name. The left side of the panel displays a list of directories where the files may be downloaded. Check the directory where you would like the files downloaded.

The right side of the panel shows the files available on the MFT Internet Server. The Server file names cannot be changed. However, you can pick and choose which files you would like to download. Click on the “Select All” button to download all the files listed.

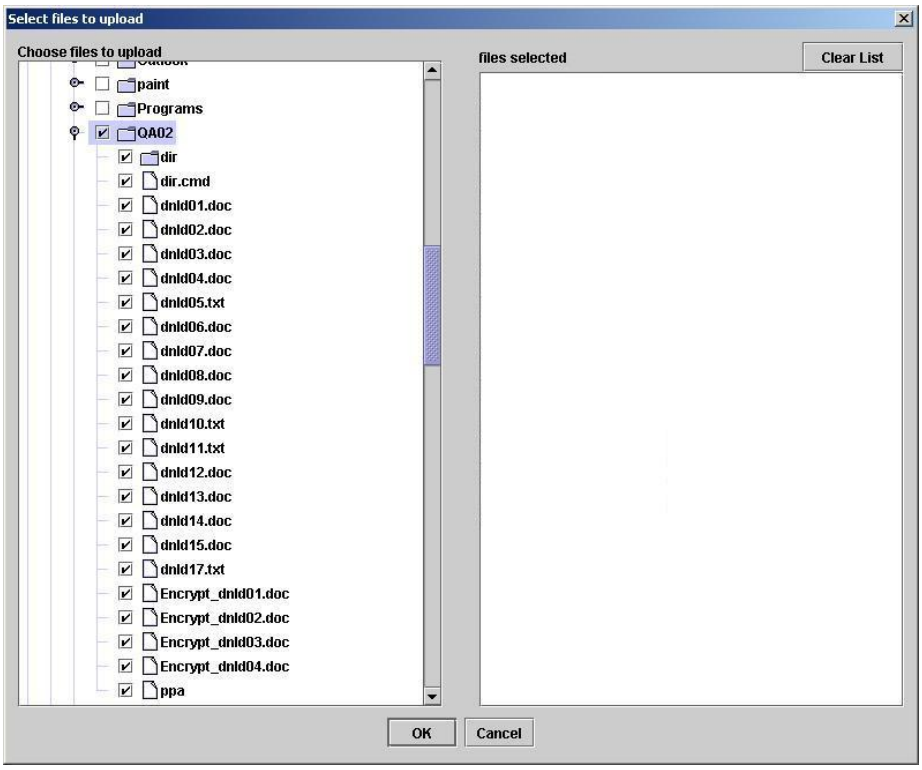


Click the OK button. This will bring you back to the Thin Client.
You should see the number of files selected to download as in the screenshot below. Click on the Download button to initiate the directory transfer.



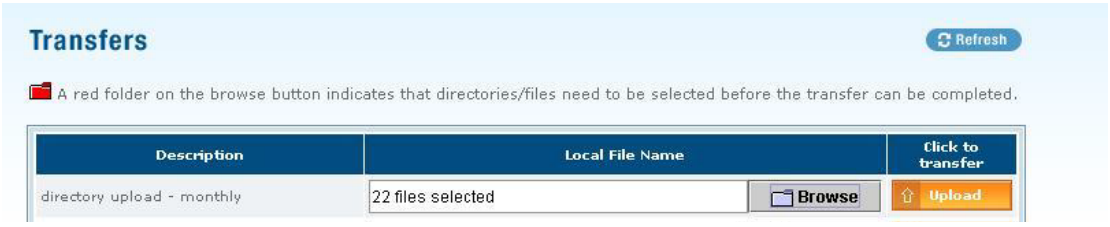
3.2.1.2 Directory Upload

In order to do an upload of a directory, click the Browse button displaying the red folder icon next to the Local File Name. The left side of the panel displays a list of directories and files to select to be uploaded. The right side of the panel will be blank.



Click the OK button. This will bring you back to the Thin Client.

The directory transfer that you browsed will now show the number of files selected. Click on the Upload button to initiate the directory transfer.



3.2.2 Directory Transfers using Platform Command Line Utility

Executing a directory transfer on the command line will work the same way as doing a single file transfer, except there are extra commands that will need to be used. An entire directory or just one file can be transferred using a directory definition. The following Internet parameters will be used in the same manner as a regular file transfer:

ListAllFiles
ListDownloadFiles
ListFile
ListUploadFiles
ProcessAllFiles
ProcessDownloadFiles
ProcessFile
ProcessUploadFiles

There are two additional parameters that need to be used:

SubDir
For Directory uploads, should MFT Internet Server scan subdirectories for files to transfer. For Directory downloads, should MFT Internet Server process data in MFT Internet Server subdirectories. When No is specified, MFT Internet Server will process files only in the defined directory. When Yes is defined, MFT Internet Server will process files in SubDirectories as well as in the defined directory. This parameter is valid only for MFT Internet Server files defined with the directory flag. It is ignored for all other requests. This parameter is supported on all List and Process calls.

FileName
This parameter is used only on Directory Download requests. It allows the user to define a single server file name to download. It is allowed only on ListFile and ProcessFile calls.

3.2.2.1 Processing for a Download Directory

- LocalFileName points to a directory or a File Name
- FileName points to the MFT Internet Server File Name
- SubDir defines whether we will process files in subdirectories.

When FileName is defined, it means that you want to process only a single file. If FileName does not point to a valid MFT Internet Server file name then the request will fail. If LocalFileName is not defined, then MFT Internet Server will store the file in the directory pointed to by the MFT Internet Server ClientFileName. If LocalFileName points to a file, then the file will be saved to that file name. If LocalFileName points to a directory, then the file will be saved to that directory using the name defined by the FileName parameter. If LocalFileName is not defined as either a file or directory, then we will assume it to be a file name. If the fully qualified file name is invalid, then the request will fail; we will not create the directory in this case.

When FileName is not defined, it means that you want to process the contents of the directory. If LocalFileName is not defined, then MFT Internet Server will store the files in the directory pointed to by the MFT Internet Server ClientFileName. If LocalFileName points to a directory, then the files will be saved to that directory using the names of the server files. If LocalFileName does not point to a directory, then we should display an error. MFT Internet Server will not create the high level directory; it must exist. If the SubDir parameter indicates that we will process directories, then we should create any subdirectories within the directory pointed to by the LocalFileName (or ClientFileName if not defined).

3.2.2.2 Processing for an Upload Directory

LocalFileName points to a directory or a File Name
SubDir defines whether we will be scanning subdirectories for files.

When LocalFileName points to a file, then MFT Internet Server will transmit that file only. When LocalFileName points to a directory, then MFT Internet Server will transmit all files within the directory.

3.3 ***Email Processing***

There are several situations where email notification occurs:

1. When a file is added to the system, email can be sent to all users configured to perform transfer of the file. For example, if you define a single user to access the file, an email can be sent to that user. If you define a Group to access the file, then emails can be sent to all users within the group.
2. When a file transfer completes – either successfully or unsuccessfully. Email can be sent to different email addresses based on whether the transfer was successful or unsuccessful. For example, you can send an email to the Accounting Department when a transfer is successful, and to the Help Desk when a transfer fails. Email can also be sent for Internet transfers as well as Platform transfers and can have multiple recipient addresses separated by coma.
3. Email can be sent as an Alert Action. When certain trigger criteria are met an email can be sent to one or several recipients. An example of such criteria would be Internet or Platform transfers, transfers to or from a particular MFT Internet Server, uploads, downloads, sends, receives, transfer success or transfer failure.
4. Email can also be sent for Platform to Platform transfers. They will be sent via the initiating MFT Platform Server system and will not use the templates defined in Command Center.

MFT Internet Server email can be configured to change the look and feel so that the emails are in any format that the customer wants. MFT Internet Server email templates are built using XML. They are simply files on the MFT Internet Server and can be changed using any text editor. There is no restriction to the number of email templates that you can define. They can be customized for individual users and companies. MFT Internet Server provides four different email templates that will be discussed later in this section.

In order to implement the email capability, you must configure the system to tell MFT Internet Server when emails must be sent. The configuration for each situation where emails are sent will now be discussed.

3.3.1 Configuring the MFT Internet Server product for Email support

In order to support sending emails, you must configure the MFT Internet Server email parameters under System Configuration on the MFT Internet Server Administrator web page. This is done under Administration > System Configuration. This will bring you to the System Configuration page. There are six fields that are used to define the parameters necessary to add email support. Only one of the parameters is required. The parameters are:

Email Admin User Id

This is an optional field. It is only required when the email server requires a user id and password. It defines the Administrator user id for the email server.

Email Admin User Pwd

This is an optional field. It is only required when the email server requires a user id and password for authentication. It defines the Administrator password for the email server.

Transfer Failure Email Template

This is an optional field. It defines the default value for the Email Failure Template. This template can be overridden by the Email Failure Template defined on the Internet Transfer definition. If a template is defined here, instead of on the Internet Transfer definition, then this template will be used. This field should be defined if you only have a single email template to be used for all unsuccessful transfers. If this field is not defined, the default email failure template will be used: cfcc\email-template\email-failure-template.xml. If the template is in the MFT Internet Server

email-template directory you can enter the file name. Otherwise, you must enter the fully qualified file name including the path.

Email Host Name

This parameter is required if you are going to make use of the email features. It defines the name of the email system; for example, emailserver.company.com. Although this field could contain an IP Address, it typically contains the IP Name of the email server at your site. If this field is not defined, then MFT Internet Server email support is disabled.

Email Host Port

This is an optional field. If this field is not defined, the default Host Port of 25 is used. This field should only be used when the email Host Port does not use the default value of 25.

Transfer Success Email Template

This is an optional field. It defines the default value for the email Success Template. This template can be overridden by the Email Success Template defined on the Internet Transfer definition. If a template is defined here, instead of on the Internet Transfer definition, then this template will be used. This field should be defined if you only have a single email template to be used for all successful transfers. If this field is not defined, the default email success template will be used: cfcc\email-template\email-success-template.xml. If the template is in the MFT Internet Server email-template directory you can enter the file name. Otherwise, you must enter the fully qualified file name including the path.

3.3.2 Transfers Added to the System

When you want to send an email to users to notify them that a transfer is available for them to execute, you must perform the following steps:

1. Define the email address within the MFT Internet Server user record for the user associated with the Transfer request. If no email address is defined in the user record, then no file notification email will be sent to that user.
2. When a transfer record is added for a user or group of users, the **File Notification Email Template** field must point to a valid email template file name. The name must exactly match the name of the template file. When processing an email template, MFT Internet Server will first look in the MFT Internet Server "…/cfcc.war/email-template" directory for the email-template file specified. If you do not specify a fully qualified name, then the email templates must be stored in this default directory. If for some reason, you want to store the email-template files in a different directory, then you would have to define the fully qualified email-template file name in the **File Notification Email Template** parameter.

Note that all users authorized to perform the transfer that have email notification addresses defined will receive email notifications that the file is ready to be transferred.

3.3.3 File Transfer Completion

You can configure MFT Internet Server to send email notification messages to authorized users upon transfer completion. Note that you can send transfer completion messages on success and/or failure. You can send the success and failure emails to different email addresses. In order to use this support, the Email Success Template and Email Failure Template parameters must be defined and the target email addresses must be defined. Here are the steps that you need to take to implement Transfer Completion notification:

1. Define the email template files. They can be defined in either the MFT Internet Server System Configuration menu or in the MFT Internet Server Internet Transfer menu. Note that if the template is defined in both places, the MFT Internet Server Internet Transfer definition overrides the MFT Internet Server System Configuration definition.

2. Define the target email addresses. Email file completion support is enabled by entering the target email address in the MFT Internet Server Internet Transfer definition Success Recipient and/or Failure Recipient fields under the Email Notification section. You can send the email notifications to several different email addresses (separated by commas). Likewise, you can choose to send notification on success but not on failure, or vice versa.

Once the configuration parameters are defined, you can run a transfer. If the transfer is successful, the email will go to the email address of the user defined by the Success Recipient field. Note that Completion email is sent only if the file transfer was actually started. If an error occurs prior to the transfer starting, no email will be sent.

3.3.4 Email Templates

There are three different types of MFT Internet Server email notification templates:
1. File Availability
2. File Transfer Completion
3. Alert

The three types of templates are configured differently, and used different XML DTD files. It is important to note that although you can change format of the Template XML files, the DTD files should **NOT** be updated by the customer. There are references in the XML files to the DTD files defined. The DTD files should be located in the same directory as the email-template XML files. If you move the XML files (for example, they are not located in the MFT Internet Server **email-template** directory), then the DTD files should be copied from the email-template directory into the directory where the XML files are located. Since the DTD files should not be changed, the format of the DTD files will not be discussed.

Both of the template types have tokens that can be used to add parameters associated with the file transfer into the email. The tokens are defined using the following format:

```
<token name=”transferdirection”/>
```

The above example defines the use of the transferdirection token that will have a value of either UPLOAD or DOWNLOAD. The tokens will be discussed along with the other information allowed in the template. The XML templates are formatted in such as way that it is easy to change the look of the email. Because of this however, only the sections of the template that are subject to change will be discussed.

3.3.4.1 File Availability Template

Below is a copy of the File Availability Template that ships with the MFT Internet Server software. This template is named: **email-notification-template.xml** and is placed by default in the MFT Internet Server **email-template** directory.

```
<?xml version="1.0"?>
<!DOCTYPE file-notification-email SYSTEM "file-notification-email.dtd">

<!-- Sample file notification template  -->

<file-notification-email>
  <sender>
         <address>cfcc@companyname.com</address>
  </sender>
  <subject>MFT Internet Server File Availability Notification</subject>
  <message>
         FileID: <token name="fileid"/>
         Transfer Direction: <token name="transferdirection"/>
         Client File Name: <token name="clientfilename"/>
         Description: <token name="description"/>
         Available Date: <token name="availabledate"/>
         Expiration Date: <token name="expirationdate"/>
```

```
        To access this file, click on the following URL:
  https://host:port/cfcc/control?view=view/filetransfer/thin/start.jsp?FileID=<token
name="fileid"/>


        To check for all available files, click on the following URL:
  https://host:port/cfcc/control?view=view/filetransfer/thin/start.jsp
        This EMAIL has been created by: MFT Internet Server (TM) by TIBCO

  </message>
</file-notification-email>
```

Each line of interest will now be discussed.

```
<!DOCTYPE file-notification-email SYSTEM "file-notification-email.dtd">
```

This line defines the DTD file associated with the XML file. The user should insure that this file exists in the same directory as the email template. If the DTD file is not in the same directory as the email template, email processing will not work.

```
<sender>
<address>cfcc@companyname.com</address>
```

This line defines the name of the email sender. The default is sender name is **cfcc@companyname.com**. This name can be changed to any appropriate email address. When the user receives an email, the data entered here will be shown as the Sender (or From). Note that some email systems require this to be a valid email address.

```
<subject>MFT Internet Server File Availability Notification</subject>
```

This defines the information that will be shown in the Subject field of the email.

```
FileID: <token name="fileid"/>
Transfer Direction: <token name="transferdirection"/>
Client File Name: <token name="clientfilename"/>
Description: <token name="description"/>
Available Date: <token name="availabledate"/>
Expiration Date: <token name="expirationdate"/>
```

These fields define information from the transfer definition that was added. When a token is included in the field, the information from the Internet Transfer definition is substituted for the token.

To access this file, click on the following URL:

```
https://host:port/cfcc/control?view=view/filetransfer/thin/start.jsp?FileID=<token
name= "fileid"/>
```

These fields define the URL that can be used by an authorized user or group of users to access the file that has been made available to transfer. If the users click on the URL, they will be brought directly to the screen where they can access the file. Note that the MFT Internet Server administrator must change the field *host:port* to point to their MFT Internet Server. If you build your own user interface, you could insert the URL to your page here as well.

To check for all available files, click on the following URL:

```
https://host:port/cfcc/control?view=view/filetransfer/thin/start.jsp
```

These fields define the URL that can be used to access all transfer definitions that are available for the user. If the users click on the URL, they will be brought directly to the screen where they can start the MFT Internet Server file transfer applet. Note that the MFT Internet Server administrator must change

the field *host:port* to point to their MFT Internet Server. If you build your own user interface, you could insert the URL to your page here as well.

3.3.4.1.1Tokens Supported in the File Availability Template

As discussed earlier, the format of a token is:

```
<token name="xxxxxxxxxx"/>
```

where "xxxxxxxxx" defines the name of the token. The following tokens are supported in the File Availability template:

fileid This is typically used in the URL to define the file name that has just been made available.

clientfilename This defines the name that has been defined for the file on the client side.

serverfilename This defines the name that has been defined for the file on the server side. This information is not usually displayed on the users screen. If the notification message is sent to a user, then we suggest not adding this field to the file availability template. If this email is sent to an internal user, you can include this token in the email.

description This defines the description that was defined for the file in the transfer record. This is an important field for the client since it can describe the contents of the file to be sent or received.

availabledate This defines the date that the file will be made available to transfer.

expirationdate This defines the date that the file will expire and be no longer valid for transfer.

transferdirection Defines whether the transfer will be an Upload (client ➔ MFT Internet Server) or a Download (client ➔ MFT Internet Server).

3.3.4.2 Transfer Completion Templates

Below is a copy of the Transfer Completion Templates that ship with the MFT Internet Server software. There are two file transfer completion templates that ship with the MFT Internet Server product: one for successful transfers and one for unsuccessful transfers. The names of the files are:

transfer-success-email-template.xml
transfer-failure-email-template.xml

Both files are located by default in the MFT Internet Server **email-template** directory. Since the two templates are essentially the same except for some comments indicating the Success or Failure of the transfer, only the Success template will be shown and discussed here.

```
<?xml version="1.0"?>
<!DOCTYPE transfer-notification-email SYSTEM "transfer-notification-email.dtd">

<!-- Sample transfer-notification-email  -->

<transfer-notification-email>
  <sender>
          <address><token name="emailsender"/></address>
  </sender>
<!--
  <recipient>
          <address><token name="recipientemailaddress"/></address>
  </recipient>
```

```
-->
  <subject>File Transfer Success Notification</subject>
  <message>
          File Transferred Successfully!!
          User: <token name="user id"/>
          Transfer Direction: <token name="transferdirection"/>
          Client File Name: <token name="clientfilename"/>
          To Server: <token name="node"/>
          Server File Name: <token name="serverfilename"/>
          Start Time: <token name="starttime"/>
          End Time: <token name="endtime"/>
          Byte Count: <token name="bytecount"/>
          Transfer Status: <token name="transferstatusmsg"/>
          Audit ID: <token name="auditid"/>
          Client IP: <token name="clientip"/>

  </message>
</transfer-notification-email>
```

Each line of interest will now be discussed.

<!DOCTYPE transfer-notification-email SYSTEM "transfer-notification-email.dtd">

This line defines the DTD file associated with the XML file. The user should insure that this file exists in the same directory as the email template. If the DTD file is not in the same directory as the email template, email processing will not work.

<sender>
<address><token name="emailsender"/></address>

This line defines the name of the email sender. The default sender email address used is defined on the System Configuration web page in the Global Settings section in the field labeled, Sender Email Address. This email address can be changed to any appropriate email Address. When the user receives an email from MFT, the data entered here will be shown as the Sender (or From).

<recipient>
<address><token name="recipientemailaddress"/></address>

This code is currently commented out. It defines the default recipient. If you define an email address in a transfer definition **Success Recipient** field this user will receive an email when a transfer is conducted successfully. If no email address is defined here none will be sent. If you would like to send an email to a specific party you can uncomment the line, by removing the XML comments, <!—from the top line and --> from the last line. Then in place of the token, <token name="recipientemailaddress"/>, you would add a recipients email address, such as, **user@xyzcompany.com**. One reason you may want to do this would be so a specific user would get all the emails when a transfer fails. This could be a technical support user in your company. To do this you would set the users id in the **transfer-failure-email-template.xml**. That way, any requests that fail would send an email to that user.

<subject>File Transfer Success Notification</subject>

This defines the information that will be shown in the Subject field of the email. In this case it indicates that the file was successfully transferred.

File Transferred Successfully!!

This is a comment that indicates the file has been transferred successfully. You can insert other comments or instructions here as well.

User: <token name="user id"/>
Transfer Direction: <token name="transferdirection"/>
Client File Name: <token name="clientfilename"/>
To Server: <token name="node"/>


```
Server File Name: <token name="serverfilename"/>
Start Time: <token name="starttime"/>
End Time: <token name="endtime"/>
Byte Count: <token name="bytecount"/>
Transfer Status: <token name="transferstatusmsg"/>
Audit ID: <token name="auditid"/>
```

These fields define information from the definition record of the file that was transferred. When a token is included in the field, the information from the Transfer definition and Audit records are substituted for the token.

3.3.4.2.1Tokens Supported in the Transfer Completion Template

As discussed earlier, the format of a token is:

```
<token name="xxxxxxxxxx"/>
```

where xxxxxxxxx defines the name of the token. The following tokens are supported in the Transfer Completion template:

auditid	This defines the audit record number associated with the file transfer request. This can be used in a URL to point to the audit record for the file that was transferred. If done correctly, you can branch directly to the Audit record for this file transfer request. It is more likely that this would be included on the Failure template than the Success Template.
bytecount	This defines the number of bytes that were transmitted during the transfer. In a successful transfer, this should match the size of the file. In an unsuccessful transfer, this number does not necessarily match the number of bytes that were transferred. It defines the number of bytes that were sent or received before an error was detected.
clientfilename	This defines the name that has been defined for the file on the client side.
endtime	This defines the time when the file transfer request completed
fileid	This is typically used in the URL to define the record Id of the file that was transferred.
node	This defines the target Server associated with the file transfer.
proxystatusmsg	This defines the last error message associated with the file transfer request. This is usually a better indication of the actual reason that caused a file transfer failure.
serverfilename	This defines the name that has been defined for the file on the server side. This is also the name of the file on the target Server.
sessionid	This defines the sessionid used for the file transfer. This is for information purposes only.
starttime	This defines the time when the file transfer request was started.
transferdirection	This defines whether the transfer will be an Upload (client ➔ MFT Internet Server) or a Download (client ← MFT Internet Server).
transferstatus	This defines the transfer status. It will say either SUCCESS or FAILURE.
transferstatusmsg	This defines the last message associated with the file transfer request. This is often a generic message that indicates that the transfer failed.
userid	This defines the user id associated with the file transfer.

3.4 ***File Tokens***

MFT Internet Server supports the use of file tokens in the server file name. When creating a file record in the MFT Internet Server database you can use any of the supported file tokens in the name. When this file is transferred the tokens will be translated to a new value within the file name.

Tokens use the following format within the file name: #(*token*)

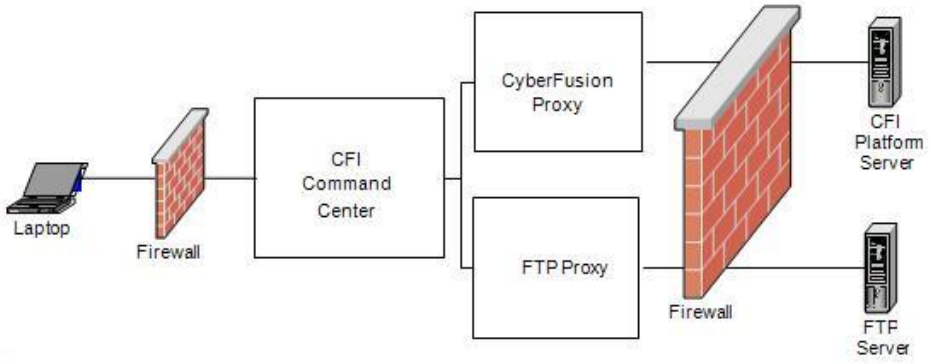
For the complete list if tokens available click on the File Token List link next to the Server File Name field of the Add Transfer web page.

3.5 FTP Proxy

MFT Internet Server no longer requires any third party software to send to a remote system that is something other than the MFT Internet Server. MFT Internet Server has been enhanced with the capability to proxy MFT Internet Server file transfers to FTP servers. This will convert HTTP data to FTP protocol in order to send data to an FTP Server. This will enable a MFT Internet Server Client to access data on many computers (nodes) within a customer site. Since almost all organizations have access to an FTP or Secure FTP server, this will also allow MFT Internet Server to push files to the client FTP Servers.

3.5.1 Description

The FTP Proxy component of MFT Internet Server allows file data to be proxied to and from servers that are not running a MFT Platform Server Responder. The following diagram shows a high level overview of the FTP Proxy component, and how it coexists with MFT Internet Server.



The FTP Proxy component provides functionality similar to the MFT Platform Server proxy component:

- File data to be transferred to/from the client does not have to reside on the MFT Internet Server.
- File data to be transferred to/from the client does not have to reside in the DMZ.
- File data is proxied using the FTP 959 specification.
- File data can be proxied to any machine running an FTP Server.
- File data can be proxied securely using an SSL connection to the FTP server.
- Directory proxies are supported, but subdirectories are not supported. (Subdirectories are supported under a MFT Platform Server directory proxy.)

To Configure MFT Internet Server to proxy to an FTP proxy:

- Create a Node with the following parameters:
  - Node Name – Name of Node
  - IP Name – IP Name/Address of the FTP Server
  - IP Port – Port number that the FTP Server is listening for connections.
  - Node Type – FTP
  - Server Type – operating system of the FTP Server (or operating system that the FTP Server is emulating)
  - Data Connection Type – This option should be configured if the FTP Proxy is having trouble transferring though a firewall.
    - PORT – FTP Proxy listens for the data portion of an FTP transaction. (Default)
    - PASV - FTP Server listens for the data portion of an FTP transaction.
  - Connection Security Type – Enables encryption when proxying to an FTP Server.
    - None – No encryption is used.
    - Explicit SSL – The FTP proxy connects to the FTP Server's unsecured port and then negotiates an SSL connection.

    - Implicit SSL – The FTP proxy makes an SSL connection to the FTP Server's secure port.
- Create a File record and specify the newly created Node for the Node Name parameter.

3.6 FTP Server

MFT Internet Server allows files to be transferred between the end user's local file system and the MFT Internet Server using FTP as the transfer protocol. This allows a MFT Internet Server end user to use virtually any FTP client to transfer files with MFT Internet Server.

MFT Internet Server FTP Server Features:
- RFC 959 Compliance
- RFC 2228 Compliance for FTP over SSL (Explicit SSL Support)
- Implicit SSL Support

When a user connects to the MFT Internet Server FTP Server, MFT Internet Server creates a Virtual Directory Structure (VDS) of files the user is allowed to transfer files through FTP. A user's VDS, maps MFT Internet Server Transfer definitions for that particular user to a directory structure more familiar to FTP users.

MFT Internet Server supports the following types of file definitions for VDS creation:
- Transfer definitions for directory download
- Transfer definitions for single file download
- Transfer definitions for directory upload

Note: MFT Internet Server file definitions for single file upload are not supported by the MFT Internet Server FTP Server and are ignored.

A MFT Internet Server Transfer definition is mapped to the user's VDS through the file definition's "Virtual Alias" parameter. The interpretation of the Virtual Alias parameter varies according to the file definitions transfer type. For instance, if the Virtual Alias parameter for a directory download file definition is set to "/files", all files (and sub-directories) represented by that particular file definition are mapped to the /files directory in the user's VDS. The user would logon to the FTP server and change to the files directory to see those files. If the Virtual Alias parameter for a single transfer file definition is set to /data.txt, the file definition is represented as /data.txt in the user's VDS. The user would see the file as data.txt in their root directory.

The Virtual Alias parameter for a directory upload file definition maps to a directory in the user's VDS to which files can be uploaded. Under this scenario a directory download file definition should also be created whose Virtual Alias matches the directory upload file definition Virtual Alias. This allows end users to upload and download from a directory in their VDS.

3.6.1 Examples

These examples show Client File Name, Server File Name and Virtual Alias parameters and how they are resolved during FTP transaction.

Let's assume that there is a directory called "c:\test1" (Client File Name) on the client's side containing files file1.txt and file2.txt. The client will perform an FTP Upload (put) and an FTP Download (get) to and from the MFT Internet Server FTP Server on 192.168.333.333. There is a directory called "c:\test2" on the MFT Internet Server (Server File Name) that contains files file3.txt and file4.txt. The transfer will be done using a user id of "user1".

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

Step1.
User "user1" performs an FTP login from the client side "c:\test1" directory onto MFT Internet Server FTP Server on 192.168.333.333. He will see the "Welcome!" message configured on the MFT Internet Server.

```
C:\test1>ftp 192.168.333.333

Connected to 192.168.333.333.

220-TIBCO Corp. MFT Internet Server FTP Server (v. 6.0)

220 This is MFT Internet Server 6.0 on 192.168.333.333 Welcome!

User (192.168.333.333:(none)): user1

331 Password required for user1

Password: ************

230 Logon OK. Proceed.
```

Step 2.
User "user1" is able to see the list of files available for the Upload and Download transactions according to File Definitions:

```
ftp> dir

drwx------    user11  user1              0 Oct 13 09:56 FtpFiles

d-wx------    user11  user1              0 Oct 13 09:56 FA1240000001

dr-x------    user11  user1              0 Oct 13 09:56 FA1240000002
```

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

Note: Files named FA1240000001 and FA1240000002 are examples of an error condition. They are shown here as an example of what the user may see when no Virtual Alias parameter is configured. They are the actual File IDs which user "user1" will see if no Virtual Alias parameter was configured for Upload (FA1240000001) or Download (FA1240000002) file definitions. We will use the correct configuration: "FtpFiles" for our example of the FTP transaction flow.

Step 3.
User “user1” performs listing of /FtpFiles directory in order to see the files available for transfer:

```
ftp> cd FtpFiles

ftp> dir

150 Opening data connection for file list.

-rwx------    user11  user1         79005 Oct 06 14:25 file3.txt

-rwx------    user11  user1         702188 Oct 06 14:42 file4.txt
```

Step 4.
User “user1” performs an Upload (put) of the file file1.txt from his current c:\test1 directory on the client side to the /FtpFiles directory on the Server side and then checks that the file was uploaded by listing the /FtpFile directory again:

```
ftp> put file1.txt

200 PORT command successful.

150 Opening data connection for FtpFiles

226 Transfer successful. AuditID=A51350000001

ftp: 40705 bytes sent in 0.00Seconds 40705000.00Kbytes/sec.

ftp> dir

-rwx------    user11  user1          40705 Oct 13 09:57 file1.txt

-rwx------    user11  user1          79005 Oct 06 14:25 file3.txt

-rwx------    user11  user1         702188 Oct 06 14:42 file4.txt
```

Step 5.
User “user1” performs Download (get) of the file3.txt down to the client side:

```
ftp> get file3.txt

150 Opening data connection for file file3.txt (79005)

226 Transfer successful. AuditID=A51350000002

ftp: 79005 bytes received in 0.88Seconds 90.29Kbytes/sec.
```

*3.7 **Multi-Language Support***

MFT Internet Server supports multiple languages for MFT Internet Server’s various File Transfer clients. This feature allows text on the web pages, as well as messages that are to be displayed to the end-user, to be displayed in various languages.

- All messages and text that are displayed to the end-user using the MFT file transfer screens will be displayed in the language preferred by that end-user. The MFT Internet Server administration screens will not support multiple languages and will be shown in English.
- All dates and times that are displayed to the end-user performing the file transfer will be displayed in the format preferred by that end user’s region (according to language). The MFT Internet Server administration screens are to be provided in U.S. format only.

- File transfer end-user messages consist of text produced by the following MFT Internet Server components:
    - File transfer applets - includes the Thin Client file transfer applet as well as the File Browse applet.
    - File transfer web pages - includes the web pages that support the Thin Client applet.
    - File Transfer Web Service - includes all error messages that are returned by the File Transfer Web Service.
    - File Transfer Servlet - includes all success and error messages that are returned by the File Transfer Servlet.
    - File Transfer Utility - includes all success and error messages that are produced by this utility.
- Trace messages produced by these components will remain in English.
- File transfer end users will communicate their preferred language to MFT Internet Server by configuring their browser and local operating system to request information in their preferred language. Note: Language preference is usually done automatically when working on an international version of Windows or can be controlled manually by setting the language preference in the browser.
- If the end user's preferred language is not one supported by MFT Internet Server, then all messages and text will be in English.
- MFT Internet Server supports the following languages:
    - English
    - French
    - Italian
    - Portuguese
    - Spanish
- Multiple language support will be performed on the machine that produces the text to be translated. In other words, language translation for JSPs and Servlets will occur on the MFT Internet Server, while language translation for applets and the File Transfer Utility will occur on the client machine.

3.8 ***Changing the DB Userid or Password***

If you need to define a new database user id and/or a database password to be used when a connection is made to the CFCC database, you must follow the following three steps.

MFT Internet Server provides a utility called dbsettings to assist you with this process. This utility enables you to update the DBUser and/or DBPass fields defined in your web server's web.xml. The utility will save the DB password in an encrypted format if desired. To use this utility, navigate to the following MFTIS installation directory:

<MFT_Install>\distribution\util****dbsettings

Run the script **dbsettings.bat** for Windows (**dbsettings.sh** for UNIX installations)

Example output is as follows:

```
* The dbsettings program allows you to configure your
* database settings contained in the application's
* web.xml file as well as encrypt the database user's
* password contained in this xml file.
*
* To make any changes to the web.xml file you will need
* to provide the full path to the web.xml file. Some
* examples are displayed for your convenience.
* To edit your database settings choose option 1 from
* the main menu and you will be given the choice to:
* update your database driver, update the database URL
* used to make a connection to the database server, update
* the database userid, or to update the database password
* which can be stored in encrypted or clear text format.
*
* Any changes made will be saved upon exiting the program
* by choosing option 2. At that time you will be asked if you
* want to save your changes.

************************************************************************
```

```
Enter the full path to the application's web.xml file. (Such as the example belo
w)

C:\MFT\server\webapps\cfcc\WEB-INF
: C:\MFT\server\webapps\cfcc\WEB-INF

Please select one of the following options:
==========================================
1. Update Database settings
2. Exit

1

Current Database Settings in web.xml
====================================
1. Driver:   oracle.jdbc.driver.OracleDriver
2. URL:      jdbc:oracle:thin:@10.97.198.82:1521:orcl
3. User ID:  QA_USER
4. DB Password: ******   Encrypted? Yes
5. Back to Main Menu

Enter the number of the setting you wish to change.
:3
Enter the database user ID (Current [QA_71])
:DBUSERID

Current Database Settings in web.xml
====================================
1. Driver:   oracle.jdbc.driver.OracleDriver
2. URL:      jdbc:oracle:thin:@10.97.198.82:1521:orcl
3. User ID:  QA_USER
4. DB Password: ******   Encrypted? Yes
5. Back to Main Menu

Enter the number of the setting you wish to change.
:5

Do you wish to encrypt the password? y or n. (Default [y])
: y

Do you wish to save your changes? y or n. (Default [n])
: y
C:\MFT\server\webapps\cfcc\WEB-INF\web.xml updated successfully
You must start and stop the server in order for changes to take affect.
```

Once you change the user id you should choose option 4 to change the password for that user id. You would save the changes and encrypt the password if you would like.

Note: For installations using an MSSQL database that will be using Windows Authentication you must add the domain parameter with the domain name to the end of the database URL. To do this you would choose option 2 and enter the new database URL, i.e., jdbc:jtds:sqlserver://10.1.2.182:1433/MFT67;domain=*DomainName*.

This concludes updating the DB Userid and Password for MFT to connect with.

5

4 Sample JMS XML

This section describes the sample JMS XML Schema files (files ending with the extension .xsd) included with MFTCC and MFTIS. We provide nine XML Schema files and 3 accompanying XML sample files. To view any of the XML Schema or XML files it is recommended to use a text editor such as Notepad or NotePad++.

4.1 JMS XML Schema and XML files

All JMS sample files can be found in the following installation directory:
<MFT_Install>/server/webapps/<context>/example/JMS.

XSD files (These files define the rules that must be followed when creating XML files and therefore should not be updated):

XML Schema File Name	Description
AuditRequest.xsd	Defines the format of the parameters necessary to initiate an Audit Search of the MFT Database. The Audit request will search the MFT database for transfers that match the defined Audit Search filters.
AuditResponse.xsd	Defines the format of the Audit Response. The Audit Response displays the results completed transfers. This xsd is used for multiple responses and returns an array of 0 or more Audit records. For Audit Search, it will return a record for each transfer that matches the Audit Search filters. For other requests, it will return only one record. The Audit Response is written in response to the following Command Center and Internet Server functions: : Alert : Audit Request : Transfer Notification : Transfer Request Internet Server : Transfer Request Platform Server
ManageConfigResponse.xsd	Defines the xml data that is returned when a ManageRequest is initiated and the Request Type is “ManageConfigRequest”. This response xml maps the MFT JMS configuration parameters.
ManageRequest.xsd	Defines the format of the parameters necessary to initiate a Management Request. This request is used internally to extract configuration information from the

	MFT Internet Server. Three Request types are allowed: : ManageConfigRequest – Returns the JMS configuration parameters : ManageServerRequest – Returns a list of MFT Servers defined to Internet Server : ManageServerTransfers – Returns a list of pre-defined Transfers Note that the ManageServerRequest will return a different list of servers based on the request JMSType set: ManageServerRequest– return all Servers defined with a Server Type of Platform Server ManageServerRequestIS– return all Servers defined with a Server Type of Internet Server
ManageServerResponse.xsd	Defines the xml data that is returned when a ManageRequest is initiated and the Request Type is “ManageServerRequest”. There are two types of responses that can be returned, based on the JMSType setting of the ManageServerRequest. : Request JSMType= ManageServerRequest. Returns the name of all Platform Servers defined to MFT Internet Server. : Request JSMType= ManageServerRequestIS. Returns the name of all Internet Servers defined to MFT Internet Server.
ManageTransferResponse.xsd	Defines the xml data that is returned when a ManageRequest is initiated, the Request Type is “ManageTransferRequest” and the request JMSType is “ManageTransferRequest”. This response returns all Platform Servers Transfers defined to MFT Internet Server.
ManageTransferResponseIS.xsd	Defines the xml data that is returned when a ManageRequest is initiated, the Request Type is “ManageTransferRequestIS” and the request JMSType is “ManageTransferRequestIS. This response returns the all Internet Servers Transfers defined to MFT Internet Server that the user defined in the ManageRequest is authorized to access.
TransferRequestInternetServer.xsd	Defines the format of the parameters required to initiate an Internet Server Transfer. Internet Server transfers can only be initiated through JMS. Internet Server transfers can perform the following actions: : Read a JMS queue and send the data to a remote destination : Read a local file and send the data to a remote destination : Read data from a remote destination and

	write data to a JMS Queue : Read data from a remote destination and write data to a local file Note that two JMS records can be returned for this request: : Immediate Response indicates whether the request has been accepted and submitted to the Internet Server for processing. This response does not have an xsd because no xml is returned with this response. All data is returned in the JMS header. : Audit Response is written when a request has been accepted and the TransferStatusCheck parameter is set to "Yes".
TransferRequestPlatformServer.xsd	Defines the format of the parameters required to initiate a Platform Server Transfer. This is sometimes called a 3rd party transfer. Internet Server picks up the data from the JMS Queue and initiates a transfer to Platform Server A to transfer a file to/from platform Server B. Note that two JMS records can be returned for this request: : Immediate Response indicates whether the request has been accepted and submitted to the Platform Server for processing. This response does not have an xsd because no xml data is returned with this response. All data is returned in the JMS header. : Audit Response is written when a request has been accepted and the TransferStatusCheck parameter is set to "Yes".

XML files: These files define the parameters necessary to perform a JMS function. We suggest that you copy these files to a new folder when you want to update them in order to keep the original files in their original state.

Sample XML File Name	Description
AuditRequest.xml	Defines sample xml data to perform an Audit Request.
TransferRequestInternetServer.xml	Defines sample xml data to initiate an Internet Server Transfer.
TransferRequestPlatformServer.xml (For MFT Command Center requests only)	Defines sample xml data to initiate a Platform Server Transfer.

Each sample xml file has a corresponding xsd file. Refer to the xsd associated with the xml for the rules that define allowable values in the xml file.

4.2 Using JMS XML files

Each .xml file has a corresponding .xsd file. We have provided three sample xml files as seen in the list above. When you want to create an accompanying .xml file for one of the .xsd Schema files refer to the element details within the .xsd.

6

5 ID Information and Field Lengths

This section is to provide you with ID Information of how a transfer is identified as well as the lengths of various fields in the MFT database.

5.1 ID Details

MFT Platform Server Internet Server assigns Ids to various functions. All the Ids have the same format except for the length of the sequential number given at the end. The Id can be broken up into the following components:

Byte	Description
1	Source of the Id: A = MFT Platform Server Internet Audit C = MFT Platform Server Platform Audit E = Alert Audit Id F = Transfer definition Id I = Initiator Audit record L = Alert Id N = Node Id P = Platform Server User Profile and Responder Profile definitions R = Responder Audit record S = Audit Search Filter definition T = Platform Server Transfer definition
2-5	Date in the format MDDY 1 – January 2 – February 3 – March 4 – April 5 – May 6 – June 7 – July 8 – August 9 – September A – October B – November C – December
6-12	Sequential number between 0 to 9999999

The sequential number at the end of the Id will only be five digits for the Initiator or Responder platform transfers. All the other Ids will contain a seven digit number.

5.2 Field Lengths

Field (Web Page)	Size
Advance Notice of Expiring Passwords (System Configuration)	2
Alert Description (Add Alerts)	256
Alert Description (Search Alerts)	256
Alert Email Address (System Configurations)	255
Alert Id (Search Alert)	12
Alias (Import FTP System Key)	64
Alias (Import SSH System Key)	64
Allocation Directory (Management – Add/Execute Platform Transfer)	8
Allocation Directory (Platform Transfer)	8
Alloc Primary (Add Transfer)	8
Alloc Primary (Management – Add/Execute Platform Transfer)	8
Alloc Primary (Platform Transfer)	8
Alloc Secondary (Add Transfer)	8
Alloc Secondary (Management – Add/Execute Platform Transfer)	8
Alloc Secondary (Platform Transfer)	8
Async Response URL (Configure AS2 Server)	255
Audit Id (Add Audit Search)	12
Audit Id (Search Audits)	12
Block Size (Add Transfer)	5
Block Size (Management – Add/Execute Platform Transfer)	5
Block Size (Platform Transfer)	5
Certificate DN (Add User)	256
Check Interval (Configure Server Status)	5
Client File Name (Add Alert)	256
Client File Name (Add Audit Search)	256
Client File Name (Add Transfer)	256
Client File Name (Internet Checkpoints)	256
Client File Name (Search Alerts)	256
Client File Name (Search Audits) (same for both)	256
Client Id (Configure JMS Service)	64
Collect History (Add Server)	4
Collection Interval (Add Server)	9
Comment (Add Alert)	64
Comment (Add Alert: JMS)	255
Common Name (Create AS2 Keys)	64
Common Name (Create FTP System Key)	64
Common Name (Create SSH System Key)	64
Community Name (Add Alert)	256
Company Name (Add User)	64
Context (System Configuration)	32
Country (Create AS2 Keys)	2
Country (Create FTP System Key)	2
Country (Create SSH System Key)	2
Data (Add Transfer) (all 4 PPA data fields)	256
Data (Management – Add/Execute Platform Transfer) (all 4 PPA data fields)	256
Data (Platform Transfer) (all 4 PPA data fields)	256
Data Class (Add Transfer)	8

Field (Web Page)	Size
Data Class (Management – Add/Execute Platform Transfer)	8
Data Class (Platform Transfer)	8
Default Collection Interval (System Configuration)	9
Default Domain (Management – Add Platform Node)	256
Default Local Trans Table (Add Server)	256
Default Password (Add Server)	32
Default Remote Trans Table (Add Server)	256
Default Server User Id (Add Transfer)	20
Default Server User Password (Add Transfer)	32
Default Server Windows Domain (Add Transfer)	256
Default User (Add Server)	32
Default Windows Domain (Add Server)	256
Department	64
Department Name (Add Department)	256
Description (Add Audit Search)	256
Description (Add FTP System Keys)	256
Description (Add Group)	64
Description (Add OnDemand Site)	64
Description (Add PGP System Keys)	256
Description (Add Server)	256
Description (Add Server Credentials)	256
Description (Add User)	64
Description (Add Transfer)	256
Description (Management - Add Platform Node)	256
Description (Management – Add/Execute Platform Transfer)	256
Description (Management – Add Platform Responder Profile)	256
Description (Management – Add Platform User Profile)	256
Description (Create AS2 Keys)	256
Description (Create FTP System Key)	256
Description (Create SSH System Key)	256
Description (Import AS2 Keys)	256
Description (Import FTP System Key)	256
Description (Import SSH System Key)	256
Description (Search Alerts)	256
Description (System Configurations)	256
Distinguished Name (Import AS2 Keys)	256
DNI Management Password (Add Server)	32
DNI Management Port (Add Server)	32
DNI Management User Id (Add Server)	32
Effective Password (Management – Add Platform Responder Profile)	256
Effective User Id (Management – Add Platform Responder Profile)	256
Elapsed Time (Add Alerts)	9
Email Address (Add User)	1024
Email Address (Configure Status Service)	100
Email Admin User Id (System Configuration)	64
Email Admin User Password (System Configuration)	64
Email Failure Template (Add Transfer)	256
Email Failure Template (System Configuration)	256
Email Host Name (System Configuration)	64
Email Host Port (System Configuration)	5
Email recipients when user adds key (System Configuration)	256
Email Success Template (Add Transfer)	256
Email Success Template (System Configuration)	256
Email Template (System Configuration)	64
Email Template File (Add Alert)	256

Field (Web Page)	Size
Embedded Word List File Name (System Configuration)	255
End Notification Message Type (Configure JMS Service)	64
Enforce Password History (System Configuration)	2
Enter the PGP Public Key in the box below (Add PGP Public Keys)	2GB
Enter the PGP Public Key in the box below (Add PGP System Keys)	2GB
Enter the PGP Secret Key in the box below (Add PGP System Keys)	2GB
Enterprise Object Id (Add Alert)	256
Excluded Word List File Name (System Configuration)	255
Expiration Days (Management – Add/Execute Platform Transfer)	256
Expiration Days (Platform Transfer)	256
External IP Address (Add Server)	16
Failure Recipient (Add Transfer)	255
Failure Recipient (Management – Add/Execute Platform Transfer)	64
Failure Recipient (Platform Transfer)	64
File Notification Email Template (Add Transfer)	256
From Date and Time (Reports - Add Audit Search Filter)	10/4
From Date and Time (Search Alerts)	10/4
From Date and Time (Search Audits) (same for both)	10/4
Virtual Alias (Add Transfer)	1024
Full Class Name (Add Alert)	256
Full Name (Add User)	256
Full Path of Command to Execute (Add Alert)	256
Group Id (Add Group)	64
Host Name/IP Address (Add OnDemand Site)	64
Incoming Password (Management – Add Platform Responder Profile)	256
Incoming User Id (Management – Add Platform Responder Profile)	256
Initiator File Name (Platform Transfer)	256
Initiator File Name (Management – Add/Execute Platform Transfer)	256
Initiator Password (Management – Add/Execute Platform Transfer)	64
Initiator Password (Platform Transfer)	64
Initiator User Id (Management – Add/Execute Platform Transfer)	64
Initiator User Id (Management – Add Platform User Profile)	256
Initiator User Id (Platform Transfer)	64
Initiator User Id (Add Platform User Profile)	256
IP Address (System Configurations)	64
IP Address (es) (Lockout Management)	1024
IP Address or IP Name (Add User)	64
IP Name	64
IP Name (Add Server)	80
IP Port (Add Server)	5
IP Port (Configure FTP Server)	5
IP Port (Configure Platform Server)	5
IP Port (Configure SSH Server)	5
IP Port (System Configuration)	5
JKS File Name (Import SSH System Key)	256
JMS Context Factory	255
JMS Server URL	64
Key Id (Manage PGP Public Keys)	64
Keystore (Configure FTP Server)	1024
Keystore Password (Configure FTP Server)	32
Keyword Password (Configure SSH Server) (same for both)	32
License Key (Add License Key)	56
LRECL (Add Transfer)	5
Local AS2 ID (Add Server)	128
Local AS2 ID (Configure AS2 Server)	128

Field (Web Page)	Size
Local Conversion Table (Management - Add Platform Node)	256
Local Transaction Id (Add Audit Search)	10
Local Transaction Id (Search Audits) (same for both)	10
Local Translation Table (Add Transfer)	256
Local Translation Table (Management – Add/Execute Platform Transfer)	256
Local Translation Table (Platform Transfer)	256
Locale (Create AS2 Keys)	64
Locale (Create FTP System Key)	64
Locale (Create SSH System Key)	64
Management Queue Name (Configure JMS Service)	512
Max Initiators (Management - Add Platform Node)	3
Max Responders (Management - Add Platform Node)	3
Max Tries (Management – Add/Execute Platform Transfer)	8
Max Tries (Platform Transfer)	8
Maximum Days Between Password Changes (System Configuration)	3
Maximum Password Length (System Configuration)	2
Message (Add Alert)	256
Message Object Id (Add Alert)	256
Mgt Class (Add Transfer)	8
Mgt Class (Management – Add/Execute Platform Transfer)	8
Mgt Class (Platform Transfer)	8
Minimum Days Between Password Changes (System Configuration)	3
Minimum Password Length (System Configuration)	2
Name (Manage PGP Public Keys)	64
Netmask (Add User)	64
Node Name (Reports – Add Audit Search Filter)	32
Node Name (Management – Add Platform Node)	32
Node Name (Management – Add Platform Responder Profile)	32
Node Name (Management – Add Platform User Profile)	32
Node Name (Search Audits) (same for both)	32
Number of Days (Reports – Add Audit Search Filter)	3
Number of Days (Search Alerts)	3
Number of Days (Search Audits) (same for both)	3
Node Name (Internet Checkpoints)	256
Organization (Create AS2 Keys)	64
Organization (Create FTP System Key)	64
Organization (Create SSH System Key)	64
Organization Unit (Create AS2 Keys)	64
Organization Unit (Create FTP System Key)	64
Organization Unit (Create SSH System Key)	64
Optional Keystore (Configure SSH Server)	1024
Parameters (Add Alert) (same for both)	256
Partner AS2 ID (Add Server)	128
Password (Add User)	32
Password (Configure JMS Service)	64
Password (Create AS2 System Key)	112
Password (Create FTP System Key)	112
Password (Import AS2 Key)	112
Password (Import FTP System Key)	112
Password (Import SSH System Key)	112
Pass Phrase (Create PGP System Keys)	112
Phone Number (Add User)	64
Platform Server Node Name (Add Alerts)	256
Platform Server Node Name (Search Alerts)	32
Primary Keystore (Configure SSH Server)	1024

Field (Web Page)	Size
Private Key Alias (Configure SSH Server) (same for both)	32
Process Name (Add Alert)	8
Process Name (Add Transfer)	8
Process Name (Reports – Add Audit Search Filter)	8
Process Name (Management – Add/Execute Platform Transfer)	8
Process Name (Platform Transfer)	8
Process Name (Search Alerts)	64
Process Name (Search Audits)	8
Proxy Host (Configure AS2 Server)	128
Proxy Password (Configure AS2 Server)	64
Proxy Port (Configure AS2 Server)	5
Proxy Transaction Id (Internet Checkpoints)	32
Proxy User Id (Configure AS2 Server)	64
Queue Connection Factory (Configure JMS Service)	64
Queue Name (Configure JMS Service) (same for both)	64
Receive URL (Configure AS2 Server)	255
Recipient (To) (Add Alert)	256
Refresh Interval	9
Remote Conversion Table (Management - Add Platform Node)	256
Remote Translation Table (Add Transfer)	256
Remote Translation Table (Management – Add/Execute Platform Transfer)	256
Remote Translation Table (Platform Transfer)	256
Remote User Id (Add Server Credential)	32
Remote User Id	32
Remote User Password (Add Server Credential)	32
Remote User Windows Domain (Add Server Credential)	256
Request Type (Configure JMS Service) (same for all)	64
Required Number of Numeric Characters (System Configuration)	2
Required Number of Special Characters (System Configuration)	2
Required Number of Unique Characters (System Configuration)	2
Responder File Name (Platform Transfer)	256
Responder File Name (Management – Add/Execute Platform Transfer)	256
Responder Host Name (Management – Add Platform Node)	256
Responder Host Name (Management – Add/Execute Platform Transfer)	256
Responder Host Name (Platform Transfer)	256
Responder IP Port (Management – Add Platform Node)	256
Responder Password (Management – Add/Execute Platform Transfer)	64
Responder Password (Platform Transfer)	64
Responder Password (Add Platform User Profile)	64
Responder Port Number (Management – Add/Execute Platform Transfer)	5
Responder User Id (Management – Add/Execute Platform Transfer)	64
Responder User Id (Management – Add Platform User Profile)	256
Responder User Id (Platform Transfer)	64
Response Type (Configure JMS Service) (same for all)	64
Restrict Download REGEX (System Configuration)	2GB
Restrict Upload REGEX (System Configuration)	2GB
Server File Name (Add Alert)	256
Server File Name (Add Transfer)	256
Server File Name (Reports - Add Audit Search Filter)	256
Server File Name (Import AS2 Keys)	256
Server File Name (Import FTP System Key)	256
Server File Name (Internet Checkpoints)	256
Server File Name (Search Audits)	256
Server File Name Prefix	256
Server Name (Add License)	256

Field (Web Page)	Size
Server Name (Add Server)	64
Server Name (Reports - Add Audit Search Filter)	64
Server Name (Search Alerts)	64
Server Name (Search Audits)	64
Site Name (Add OnDemand Site)	64
SNMP Agent IP (Add Alert)	80
SNMP Server IP (Add Alert)	80
Socket Timeout (Configure Platform Server)	5
Specific Trap Id (Add Alert)	5
SSL Port (Configure FTP Server)	5
Start Notification Message Type (Configure JMS Service)	64
State (Create AS2 Keys)	2
State (Create FTP System Key)	2
State (Create SSH System Key)	2
Storage Class (Add Transfer)	8
Storage Class (Management – Add/Execute Platform Transfer)	8
Storage Class (Platform Transfer)	8
Success Recipient (Add Transfer)	255
Success Recipient (Management – Add/Execute Platform Transfer)	64
Success Recipient (Platform Transfer)	64
Template File for Additional Criteria (Add Alert)	256
Timeout (Add Server)	5
To Date and Time (Reports – Add Audit Search Filter)	10/4
To Date and Time (Search Alerts)	10/4
To Date and Time (Search Audits) (same for both)	10/4
Topic Connection Factory (Configure JMS Service)	64
Topic Name (Configure JMS Service) (same for both)	64
Transaction Id (Internet Checkpoints)	256
Transfer Description (Add Alert)	256
Transfer Description (Search Alerts)	256
Transfer Id (Internet Checkpoints)	12
Transfer User Id (Add Alert)	64
Transfer User Id (Audit Search)	32
Transfer User Id (Reports – Add Audit Search Filter)	32
Transfer User Id (Search Alerts)	32
Transfer User Id (Search Audits) (same for both)	32
Trap Port (Add Alert)	5
Type (Add Alert)	64
Unit (Add Transfer)	8
Unit (Management – Add/Execute Platform Transfer)	8
Unit (Platform Transfer)	8
Unix File Permissions (Add Transfer)	3
Unix File Permissions (Management – Add/Execute Platform Transfer)	3
Unix File Permissions (Platform Transfer)	3
User Id (Add User)	64
User Id (Internet Checkpoints)	32
User Id (LDAP Sync)	64
User Data (Add Transfer)	25
User Data (Reports – Add Audit Search Filter)	25
User Data (Management – Add/Execute Platform Transfer)	25
User Data (Platform Transfer)	25
User Data (Search Audits)	25
User Name (Configure JMS Service)	64

Field (Web Page)	Size
Volume (Add Transfer)	6
Volume (Management – Add/Execute Platform Transfer)	6
Volume (Platform Transfer)	6
Welcome Message (Configure FTP Server)	1024

Index

