TIBCO® Managed File Transfer Internet Server User's Guide

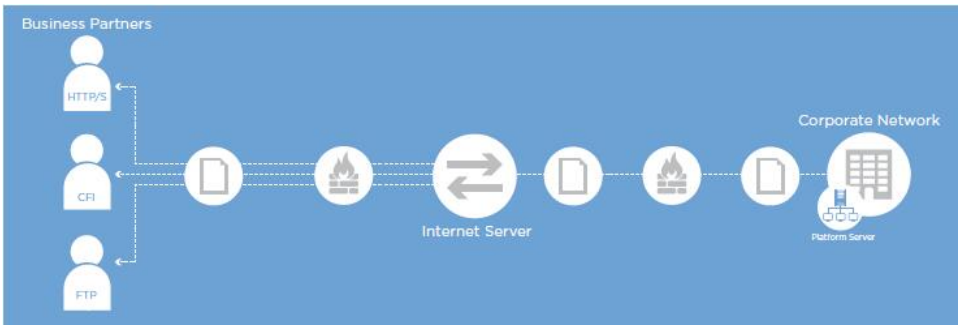
Version 8.3.2

April 2022

Contents

Product Overview

A core component of TIBCO Managed File Transfer universal solution for secure, fast file transfers, TIBCO® Managed File Transfer Internet Server is the portal or gateway through which all files are exchanged with external users.



Available as either a web service or stand-alone application, TIBCO Managed File Transfer (MFT) Internet Server enables you to integrate seamlessly with your entire B2B network, automating and simplifying the most critical data-transfer activities, and guaranteeing FTP delivery — every single time. Equally important, the product's advanced security mechanisms eliminate common authentication, security, and control risks associated with Internet file delivery.

TIBCO MFT Internet Server supports real-time communication and integration using a variety of popular protocols such as HTTPS, HTTP, FTPS (SSL), SFTP (SSH), FTP, and AS2, as well as popular open standards such as XML, SOAP, and UDDI. The solution is also incredibly easy to use. It installs quickly, is completely intuitive, and customizes easily to ensure smooth integration with your business ecosystem. To cap it all, TIBCO MFT Internet Server makes it easier to do business with your company; all your partners need is a standard web browser (no client software required).

Security

Supplies complete data security and support for the world's most stringent encryption standards.

Compliance

Ensures compliance with all major regulatory mandates (Sarbanes-Oxley, PCI-DSS, HIPAA, Gramm-Leach-Bliley, Fips 140-2, Section 508, etc.)

Guaranteed Delivery

Checkpoint/restart and other mechanisms provide guaranteed delivery and detect if a connection drops. Checkpoint/restart resumes the transfer at the exact point it dropped and continues until completed — no manual intervention is required. This provides vital support for organizations needing to satisfy service-level agreements.

High Availability/Clustering

Supports clustering for failover support and reliability.

No File-size Limits

Differs from many other file-transfer solutions because it has no file-size limitations, and can handle the transfer of very large files at the highest volumes.

Multi-Protocol

Fully supports HTTP, HTTPS, FTP, FTPS (SSL), SFTP (SSH), AS2, CFI Protocol.

Platform Agnostic/Browser-based

Allows control through any standard web browser (IE, Firefox, Safari).

Partner Integration

Helps drive your B2B integration strategy and enables your organization to connect securely and efficiently with suppliers, business partners, and customers.

No “Store and Forward”

Provides strong proxying capabilities to ensure that incoming data is delivered directly to the back-end system and never stored in the DMZ.

Easy to Use

Browser interface allows getting up and running quickly with little or no technical expertise.

Administrator Browser Configuration

You can use the administrator web pages to configure TIBCO MFT Internet Server for use.

Accessing TIBCO MFT Internet Server Administrator Browser

After TIBCO MFT Internet Server is installed and configured, you can access the TIBCO MFT Internet Server administrator web pages.

Prerequisites

TIBCO MFT Internet Server is installed without the administrator web pages by default. Ensure that you have installed the administrator service for TIBCO MFT Internet Server during the installation.

Procedure

1. Open a web browser and go to https://*[DNS_HostName]*:*[httpsPort]*/cfcc/control?view=view/admin/start.jsp.
   The DNS host name and port are configured during the installation. The default port is `7443`.
2. On the sign-on page, enter the user name and password, and then click **Sign On**.
   The default user name and password are `admin` and `changeit`.

Result

The TIBCO MFT Internet Server main web page is displayed.

Transfers

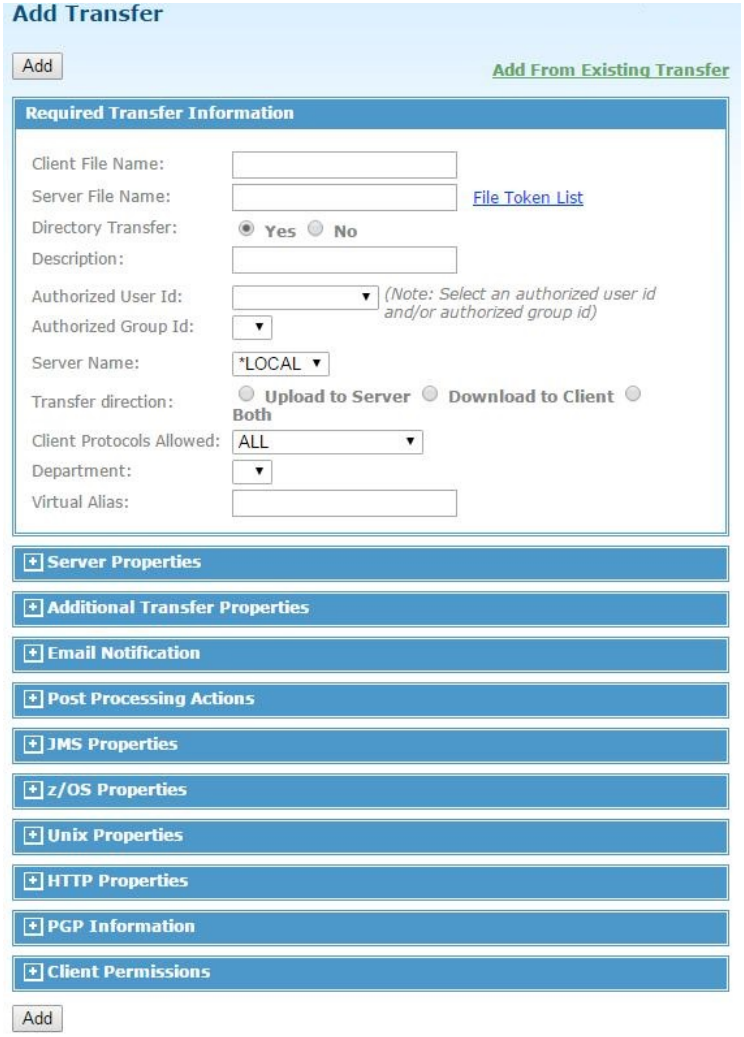
With the **Transfers** option, you can add and manage transfer definitions and on-demand sites.

Add Transfer

Click **Transfers** > **Add Transfer** to add transfer definitions on the Add Transfer page.

When a transfer user signs on to TIBCO MFT Internet Server using various clients, the transfers that will be displayed will depend on what was defined on the Add Transfer page. For more information about how to configure the fields on this page, see the online help page.

Administrative users must have AdministratorRight or UpdateTransferDefinitionRight to add a transfer definition.



The Add Transfer page contains the following sections:

- Required Transfer Information
- Server Properties
- Additional Transfer Properties
- Email Notification
- Post Processing Actions

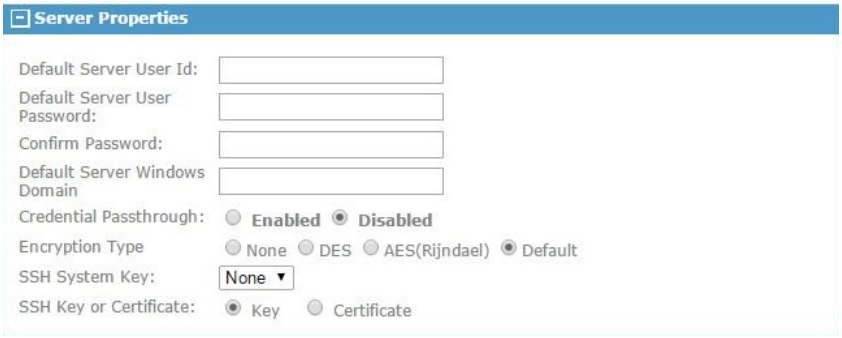
- JMS Properties
- z/OS Properties
- Unix Properties
- HTTP Properties
- PGP Information
- Client Permissions

Required Transfer Information

This section defines the parameters that are required to create a transfer record.

Server Properties

This section defines parameters specific to the server selected in the Required Transfer Information section.

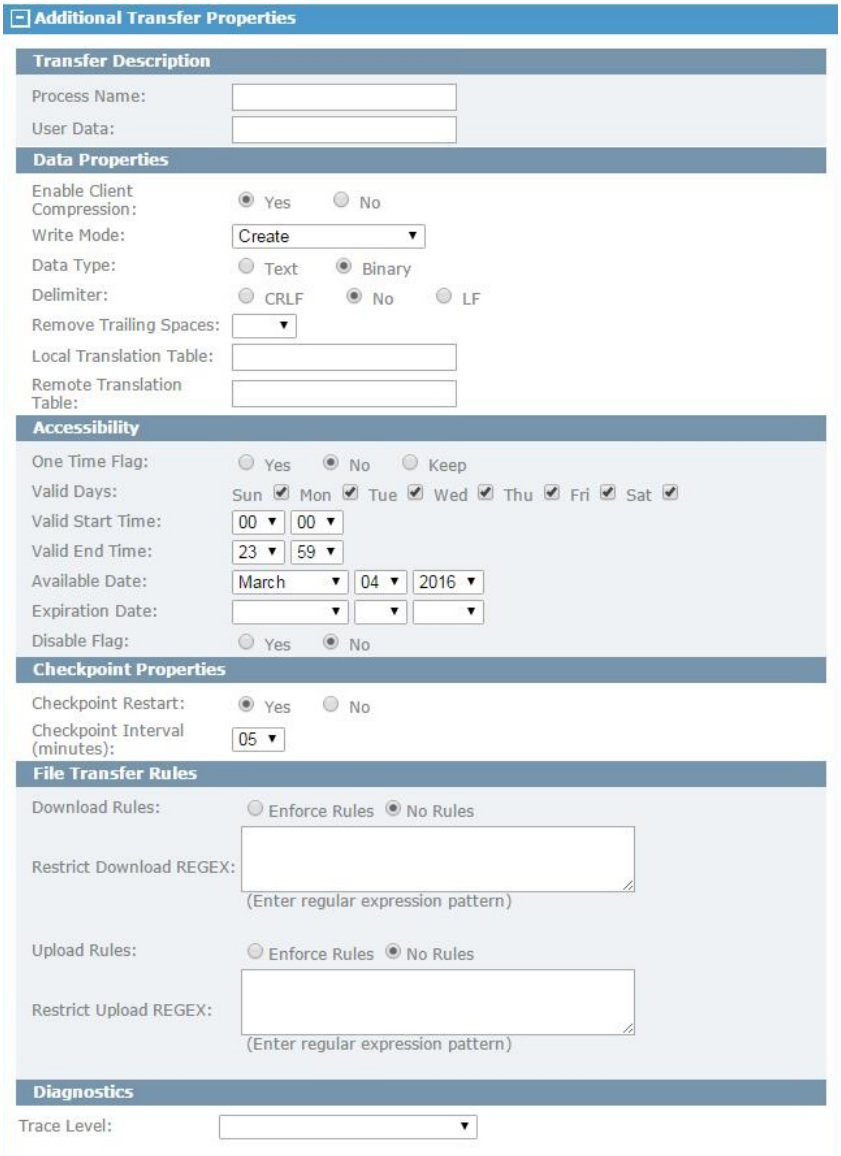


Additional Transfer Properties

This section contains 5 subsections: Transfer description, Data Properties, Accessibility, Checkpoint Properties, File Transfer Rules and Diagnostics.

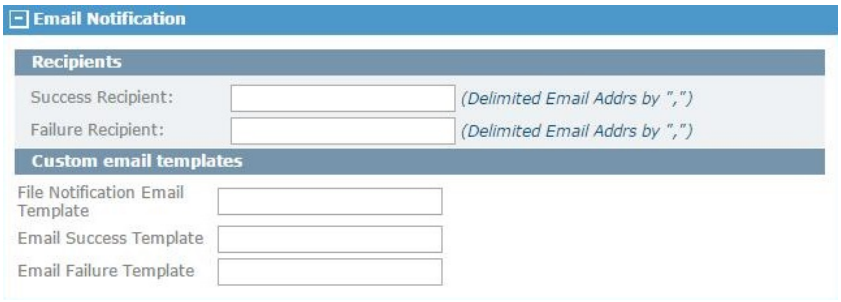
The **Checkpoint Restart** area is not supported when using PGP encryption or transfer to/from an AS2 server, and **No** should be selected.

The Write Mode is used for upload transfer definitions only; it is ignored for download transfer definitions. For uploads, it is ignored when the server associated with the transfer definition has a server type of HTTP.



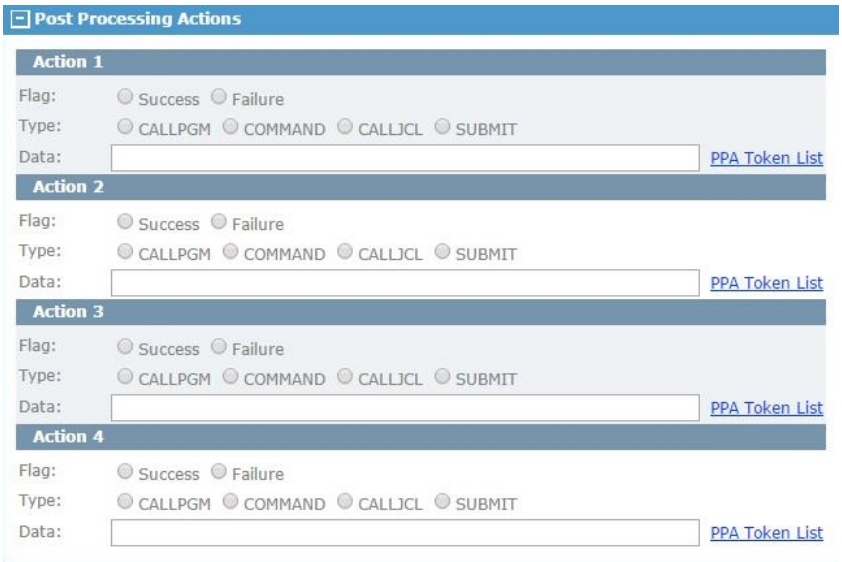
Email Notification

This section allows TIBCO MFT Internet Server to send email notification to one or more users.



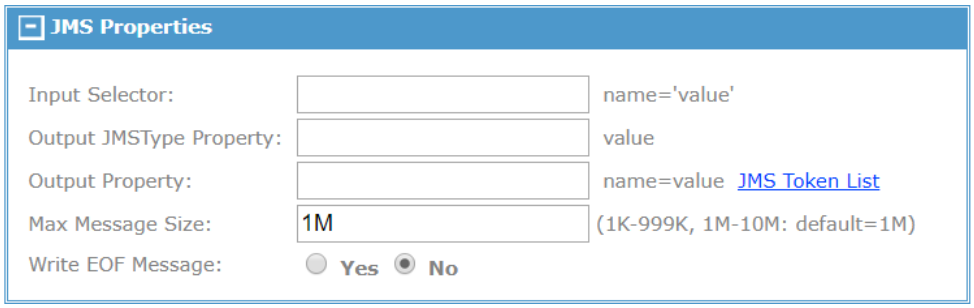
Post Processing Actions

This section allows you to perform up to four actions to be completed by the server when a file transfer request has completed.



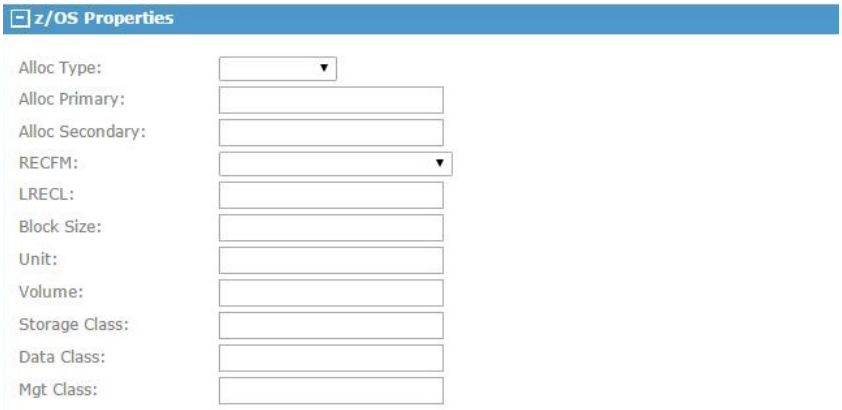
JMS Properties

This section define parameters used when the transfer definition points to a server defined with the server type of JMS. These parameters are only used when reading from or writing to a JMS queue and are ignored for other server types.



z/OS Properties

This section is used only when creating a file on a z/OS operating system through an Upload operation. You can use these parameters to define information about the file to be created.

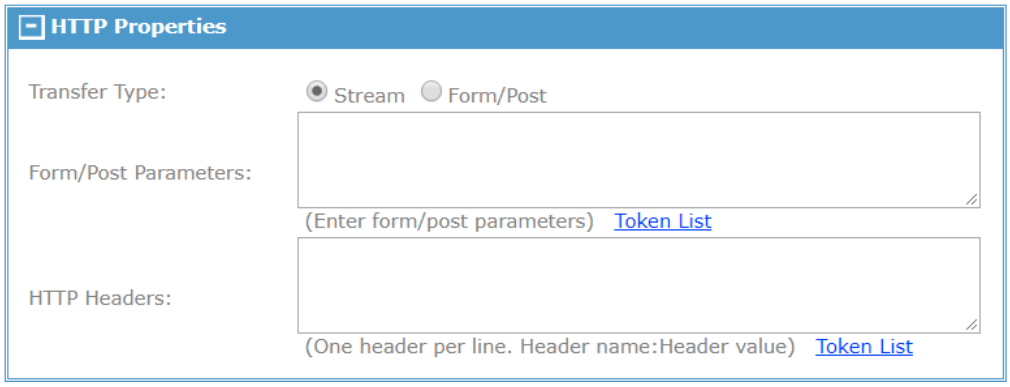


Unix Properties

This section is used only when creating a file on a UNIX operating system through an Upload operation.

HTTP Properties

This section is used only when performing a Form upload to a target HTTP server.



PGP Information

This section defines the PGP information that can be associated with a transfer.

Client Permissions

This section defines the permissions that are allowed when conducting this transfer using an HTTP, FTP, SSH, Platform Server or desktop client.

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

When specifying the **Allow Delete** or **Allow Rename** area, the server platform must be defined to the correct operating system in the server definition for proper functionality.

Add From Existing Transfer

On the Add transfer page, click **Add From Existing Transfer** to copy a transfer definition to create a new one without having to enter all the transfer information again.

After clicking **Add From Existing Transfer**, a listing of existing transfers will be displayed. Click the transfer 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 the server properties, the server user ID and password will also be blank. You have to provide the user ID and password type information for each new transfer defined.

For more information about how to configure the fields on this page, see the online help page.

Manage Transfers

Click **Transfers** > **Manage Transfers** to manage transfer definitions on the Manage Transfers page.

Users must have AdministratorRight or UpdateTransferDefinitionRight to manage transfer definitions. For more information about how to configure the fields on this page, see the online help page.

On the Manage Transfers page, you can list, search, update and delete transfer definitions.

The Manage Transfers page contains a section, Selection Criteria, and a list of the first 100 defined transfers. If there are more than 100 transfers defined, click **List Next 100 >** to access the next 100 transfer definitions. You also can click **Back** to see the previous definitions.

A list of particular transfers can be obtained by either clicking **List Transfers by Users** or entering the search criteria for any combination of transfer ID, server file name, description, authorized user ID, authorized group ID, server name and department. A percent sign (%) can be used as a wildcard character.

Clicking **List Transfers by User** will give you a list of users. Click the user ID for a listing of transfer definitions for that particular user.

To update a transfer definition, click the transfer ID of the Transfer definition that you want to change. When the changes are made, click **Update** to update the definition.

To delete a transfer definition, select the check box next to the transfer that you want to delete and click **Delete**. Multiple transfer definitions can 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 page and click **Manage Transfers**.

OnDemand

With the **Transfers** > **OnDemand** option, you can add and manage the on-demand sites.

When you want to allow end users that are using the TIBCO MFT Internet Server desktop client 7.1 or later to directly connect to a remote FTP, SSH, or Platform Server server, you would configure those servers details here. The users or departments that you authorize to connect to these servers will have an added menu item displayed in their TIBCO MFT Internet Server **Desktop Client File** menu called **Site Manager**. See *TIBCO MFT Internet Server Desktop Client User's Guide* for more information about the **Site Manager** item.

Users must have AdministratorRight or UpdateOnDemandRight to add or manage the on-demand sites to TIBCO MFT Command Center and TIBCO MFT Internet Server.

Add OnDemand Site

Click **Transfers** > **OnDemand** > **Add OnDemand Site** to add on-demand site definitions on the Add OnDemand Site page.

By default, there are no users defined to the on-demand site settings. Users must be assiged with OnDemandTransferRight before they will be displayed in the **User Ids** list.

You can select **All Users** in the **User Ids** list to allow all users with OnDemandTransferRight to connect to this server.

For more information about how to configure the fields on this page, see the online help page.

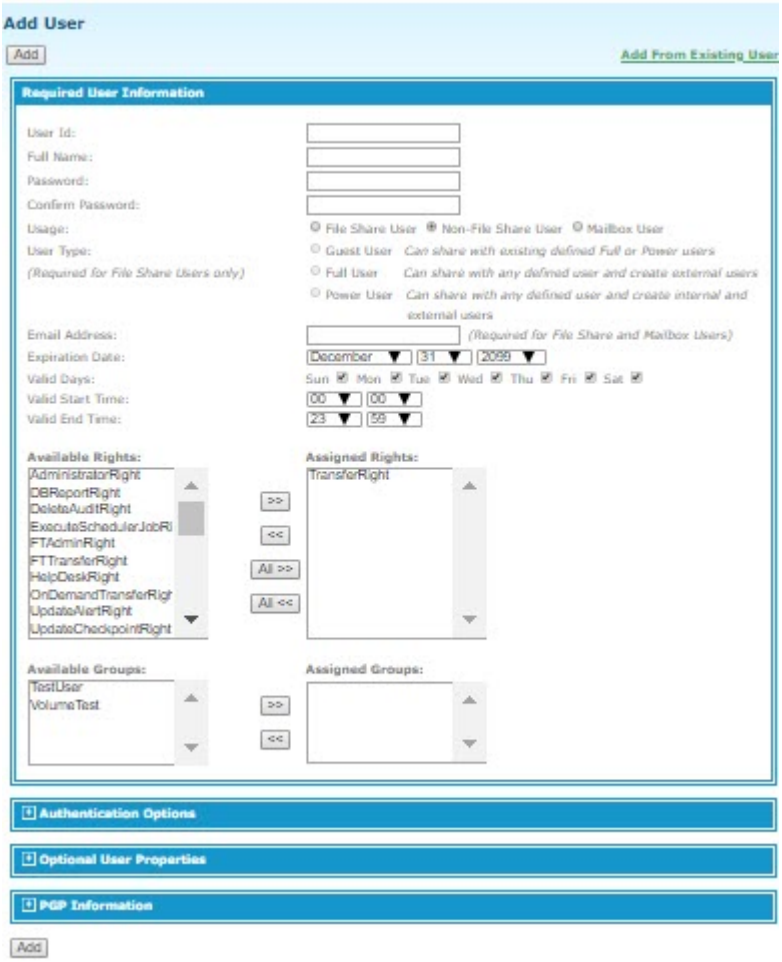
Users

With the **Users** option, you can add and manage users, transfer groups and departments.

Add User

Click **Users** > **Add User** to add user definitions on the Add User page.

Administrative users must have AdministratorRight or UpdateTransferUserRight to add a user definition.



The Add User page contains the following sections:

- Required User Information
- Authentication Options
- Optional User Properties
- PGP Information

Required User Information

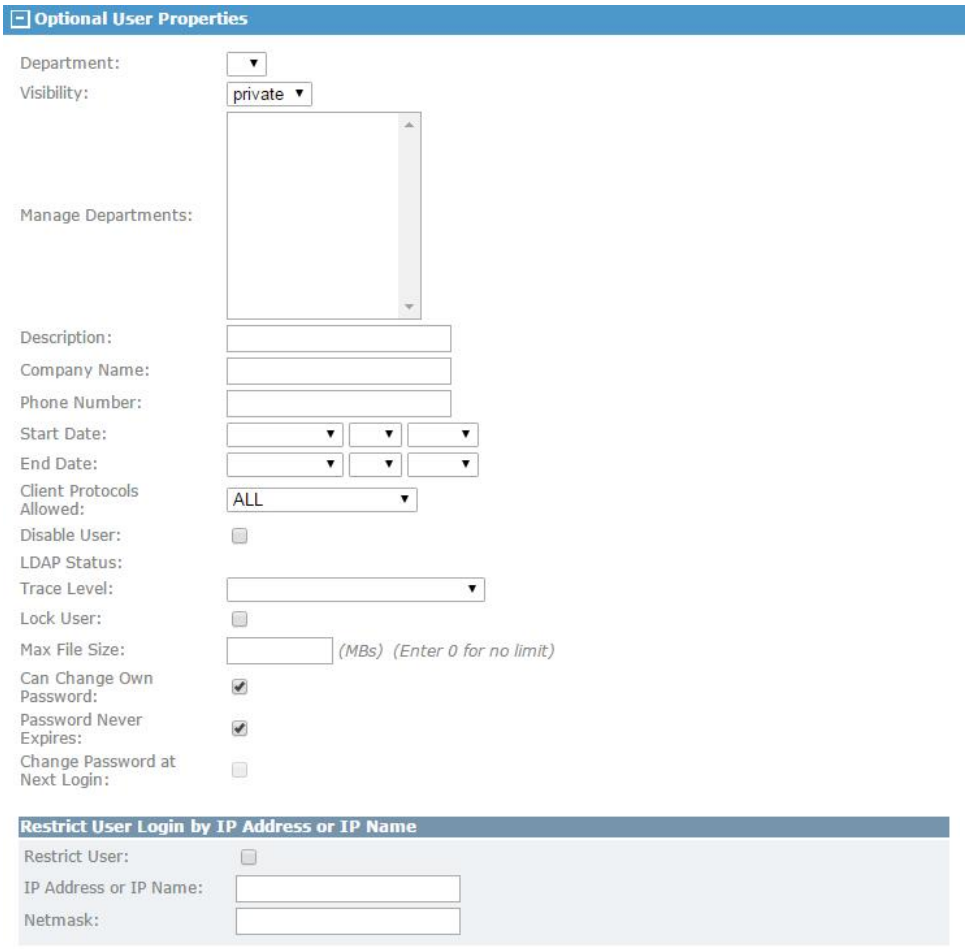
This section defines the parameters that are required to create a user record.

Authentication Options

This section defines a user client authentication method for FTP, SSH, HTTPS, and Platform Server client connections. These settings will override the global settings on the System Configuration page. You need to configure the **Certificate DN** field when trusted certificates are being added through the Administration > Protocol Keys > Trusted Certificates > Add Trusted Certificates page.

Optional User Properties

This section defines the parameters that are not required.



PGP Information

This section defines the PGP information that can be configured for the user.

By default, the ability to add a PGP public key to Internet Server will be determined by the **Allow users to add PGP Keys** area on the System Configuration page. For more information, see System Configuration. You can click **Yes** to allow the user to add PGP public keys to the MFT database.

Add From Existing User

On the Add User page, click **Add From Existing User** to copy the pre-existing user definition to create a new user definition.

For users that want to be able to use TIBCO MFT Internet Server to transfer files, their user IDs must be added to the TIBCO MFT Internet Server database.

Part of the TIBCO MFT Internet Server installation process adds 5 template users automatically to the database.

By clicking **Add From Existing User**, a listing of those pre-existing users will be displayed. Simply click one of the user IDs to copy the pre-existing user 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. Click **Add** when you are finished to have the new user added to the database. You also can edit any of the pre-existing user definitions before clicking **Add** if you want.

As new user definitions are added more template user definitions are available to choose from.

The following table lists the default template users and their assigned rights:

Template User IDs	Rights Assigned
ArchiveUser	No Rights Assigned
AS2TraceUser	No Rights Assigned
AuditorUser	ViewAlertRight ViewAuditRight ViewGroupRight ViewServerCredentialRight ViewServerRight ViewTransferDefinitionRight ViewUserRight
Collector	No Rights Assigned
HelpDeskUser	HelpDeskRight UpdateSessionRight ViewAlertRight ViewAuditRight ViewGroupRight ViewUserRight
Scheduler	DeleteAuditRight ViewAuditRight
TransferUser	TransferRight
admin	AdministratorRight TransferRight

The Collector and ArchiveUser IDs are also added by default. These IDs are used to create server credentials for the servers that will also have the enabled collection and archive option. There are no rights given to these IDs.

If you do not want to use any of the template user definitions available to you, a new user definition can be created manually.

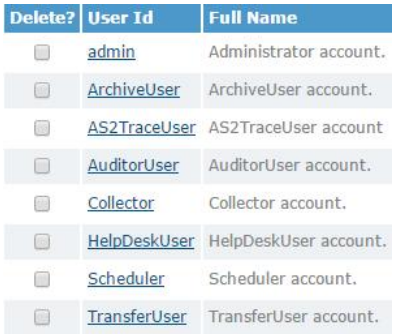
Manage Users

Click **Users** > **Manage Users** to manage user definitions on the Manage Users page.

Users must have AdministratorRight or UpdateTransferUserRight to manage user definitions. For more information about how to configure the fields on this page, see the online help page.

On the Manage Users page, you can list, search, update and delete the user.

The following figure shows the Manage Users page with the 8 template users that are automatically added to the database during the TIBCO 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 **List Next 100 >** to access the next 100 user definitions. You also can click **Back** to see the previous definitions.



Delete?	User Id	Full Name
☐	admin	Administrator account.
☐	ArchiveUser	ArchiveUser account.
☐	AS2TraceUser	AS2TraceUser account
☐	AuditorUser	AuditorUser account.
☐	Collector	Collector account.
☐	HelpDeskUser	HelpDeskUser account.
☐	Scheduler	Scheduler account.
☐	TransferUser	TransferUser account.

A list of particular users can be obtained by entering the search criteria for any combination of user ID, full name, role, group and department. A percent sign (%) can be used as a wildcard character.

To update a user definition, click on the user ID of the user definition that you want to change. When the changes are made, click **Update** to update the definition.

To delete a user definition, select the check box next to the user that you want to delete and click **Delete**. Multiple user definitions can be deleted at one time.

To refresh the **Manage Users** list, you can use the navigation box on the left portion of the page and click **Manage Users**.

Available Rights

TIBCO MFT Internet Server has granular rights that can be assigned to a user.

The following table lists the 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 TIBCO Managed File Transfer (MFT) Command Center 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 his own department and the departments that the user can manage. This right does not include TransferRight or FTTransferRight or any functions that correspond to these rights. The department administrator cannot update servers or server Credentials unless given UpdateServerRight and UpdateServerCredentialRight.

Right	Description	Description using Delegated Administration
DBReportRight	Allows a user to login and view and generate TIBCO MFT Command Center's database reports through the **Reports** > **Database Reports** option.	Allows a user to login and view and generate TIBCO MFT Command Center's database reports through the **Reports** > **Database Reports** option.
DeleteAuditRight	Allows any user to delete audit record.	Allows any user to delete audit record. Department checking will not be done.
ExecuteSchedulerJobRight	Allows a user to view and execute a job through the **Execute Now** button and Platform Server command.  This right does not allow to update a job.	Allows a user to view and execute a job through the **Execute Now** button and Platform Server command.  This right does not allow to update a job.
FTAdminAlterRight	With this right, you can view and cancel active Platform Server transfers.  This right applies only for TIBCO MFT Command Center.	With this right, you can view and cancel active Platform Server transfers. You can cancel active Platform Server transfers only if you have this right.
FTAdminRight	With this right, you can view or update Platform Transfers defined to Command Center. If this right is assigned along with ViewServerRight, you can also view and update all the items in the **Management** > **Manage Platform Functions** option. A user with only FTAdmin right cannot execute Platform Server transfers.  A user without FTAdminRight or FTTransferRight cannot add, view, or update Platform Server transfers.  This right applies only for TIBCO MFT Command Center.	With this right, you can view and update menu items from the **Management** > **Platform Transfers** option; however, you cannot execute Platform transfers. If this right is assigned along with ViewServerRight, you can also view and update all the items in the **Management** > **Manage Platform Functions** option.

Right	Description	Description using Delegated Administration
FTTransferRight	With this right, you can view and execute Platform Transfers defined to Command Center.  A user with FTTransferRight can only execute Platform Server transfers but cannot update the Platform Server transfers. A user without FTAdminRight or FTTransferRight cannot add, view, or update Platform Server transfers.  This right applies only for TIBCO MFT Command Center.	With this right, you can view and execute menu items from the **Management** > **Platform Transfers** option; however, you cannot update Platform transfers.
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** menu item to setup and conduct on-demand transfers.	Allows a user the ability to use the desktop client **Site Manager** menu item to setup and conduct on-demand transfers.
TransferRight	Allows a user to execute TIBCO MFT Command Center's Internet transfers.	Allows a user to execute TIBCO MFT Command Center's 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.
UpdateCheckpointRight	Allows a user to access the TIBCO MFT Internet Server checkpoints web page and delete checkpoints taken.	Allows a user to access the TIBCO MFT Internet Server checkpoints web page and delete checkpoints taken.
UpdateFTTransferRight	Allows a user to update platform transfer defined tthorugh the **Management** > **Platform Transfers** > **Manage Platform Transfers** option. This right will not allow the user to execute platform transfers.	Allows a user to update platform transfer defined through the **Management** > **Platform Transfers** > **Manage Platform Transfers** option. This right will not allow the user to execute platform transfers.
UpdateGroupRight	Allows a user to view and update TIBCO MFT Command Center's group records.	Allows a user to view and update TIBCO MFT Command Center's group records.

Right	Description	Description using Delegated Administration
UpdateOnDemandRight	Allows a user the ability to add or remove the on-demand sites.	Allows a user the ability to add or remove the on-demand 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 TIBCO MFT Command Center's PGP system keys.	Allows a user to add and manage the configurations of TIBCO MFT Command Center's PGP system keys.
UpdatePublicKeyRight	Allows a user to add and manage the configurations of FTPS, SFTP, Platform Server, and HTTPS public keys.	Allows a user to add and manage the configurations of FTPS, SFTP, Platform Server, and HTTPS public keys.
UpdateSchedulerRight	Allows a user to add and manage the Scheduler jobs in TIBCO MFT Command Center.	Allows a user to add and manage the Scheduler jobs in TIBCO MFT Command Center.
UpdateServerCredentialRight	Allows a user to view or update TIBCO MFT Command Center server credential records.	Allows a user to view or update TIBCO MFT Command Center server credential records.
UpdateServerRight	Allows a user to view or update TIBCO MFT Command Center server records.	Allows a user to view or update TIBCO MFT Command Center server records in his 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 AS2, FTP, SFTP, Platform SSL, HTTPS and SAML system keys system keys through the **Administration** > **Protocol Keys** > **System Keys** option. Allows a user to add and manage the configurations of Kerberos KeyTab files through the **Administration** > **Protocol Keys** > **Kerberos KeyTabs** option.	Allows a user to add and manage the configurations of AS2, FTP, SFTP, Platform SSL, HTTPS and SAML system keys through the **Administration** > **Protocol Keys** > **System Keys** option. Allows a user to add and manage the configurations of Kerberos KeyTab files through the **Administration** > **Protocol Keys** > **Kerberos KeyTabs** option.v
UpdateTransferDefinitionRight	Allows a user to view and update TIBCO MFT Command Center internet transfer definitions.	Allows a user to view and update TIBCO MFT Command Center internet transfer definitions.

Right	Description	Description using Delegated Administration
UpdateTransferUserRight	Allows a user to view and update TIBCO MFT Command Center 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.  When assigning this right to a user, you must also assign either ViewGroupRight or UpdateGroupRight.	Allows a user to view and update TIBCO MFT Command Center user records. Only 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 his own department, except UpdateServerRight and UpdateServerCredentialRight.  When assigning this right to a user, you must also assign either ViewGroupRight or 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 filters.	Allows a user to view audit records and update the audit search filters.
ViewCheckpointRight	Allows a user to access the TIBCO MFT Command Center Internet Checkpoints page and view checkpoints taken.	Allows a user to access the TIBCO MFT Command Center Internet Checkpoints page and view checkpoints taken.
ViewFTTransferRight	Allows a user to view platform Transfers defined through the **Management** > **Platform Transfers** > **Manage Platform Transfers** option. This right will not allow the user to add, update, or execute platform transfers.	Allows a user to view platform Transfers defined through the **Management** > **Platform Transfers** > **Manage Platform Transfers** option. This right will not allow the user to add, update, or execute platform transfers.
ViewGroupRight	Allows a user to view TIBCO MFT Command Center group records.	Allows a user to view TIBCO MFT Command Center group records.
ViewOnDemandRight	Allows a user to view TIBCO MFT Command Center on-demand site records.	Allows a user to view TIBCO MFT Command Center on-demand site records.
ViewPCILogRight	Allows the user to view Admin change reports.	Allows the user to view Admin change reports.
ViewPGPKeyRight	Allows a user to view PGP public keys.	Allows a user to view PGP public keys.
ViewPublicKeyRight	Allows a user to view TIBCO MFT Command Center FTP, SSH, HTTPS public keys.	Allows a user to view TIBCO MFT Command Center FTP, SSH, HTTPS public keys.

Right	Description	Description using Delegated Administration
ViewSchedulerRight	Allows a user to view the scheduled transactions.	Allows a user to view the scheduled transactions.
ViewServerCredentialRight	Allows a user to view TIBCO MFT Command Center server profile records.	Allows a user to view TIBCO MFT Command Center's server profile records.
ViewServerRight	Allows a user to view TIBCO MFT Command Center server records.	Allows a user to view TIBCO MFT Command Center's 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 Internet Server transfer records of TIBCO MFT Command Center.	Allows a user to view Internet Server transfer records of TIBCO MFT Command Center.
ViewUserRight	Allows a user to view TIBCO MFT Command Center user records and the rights associated with those users.	Allows a user to view TIBCO MFT Command Center user records and the rights associated with those users.

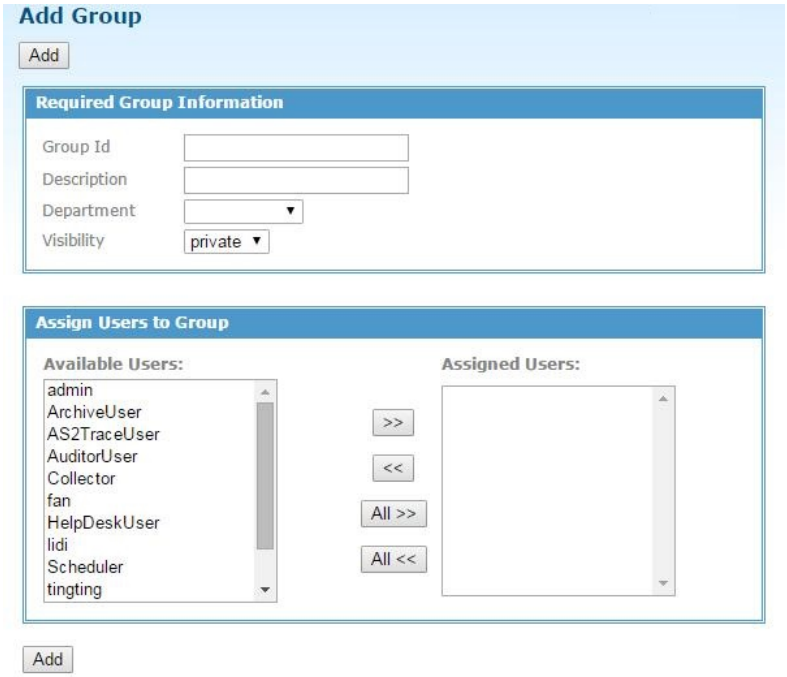
Transfer Groups

With the **Users** > **Transfer Groups** option, you can add and manage the transfer groups.

Add Group

Click **Users** > **Transfer Groups** > **Add Group** to add group definitions on the Add Group page.

This page enables administrative users to add new groups to the system. Administrative users must have AdministratorRight or UpdateGroupRight to add a group definition.



The Add Group page contains the following sections:

- Required Group Information
- Assign Users to Group

Required Group Information

This section defines parameters that are required to create a group record.

Assign Users to Group

This section defines which users will be in the defined group.

Manage Groups

Click **Users** > **Transfer Groups** > **Manage Groups** to manage user definitions on the Manage Groups page.

Administrative users must have AdministratorRight or UpdateGroupRight to manage group definitions.

On the Manage Groups page, you can list, delete and update the group definitions.

The following figure shows an example of 6 groups that had been created and can be managed from this page. The page will contain a list of the first 100 defined groups. If there are more than 100 groups defined, click **List Next 100 >** to access the next 100 group definitions. You can also click **Back** to see the previous definitions.

Delete?	Group Id	Description	Department	Visibility
☐	Accounting Group	Accounting Group	Accounting	private
☐	Help Desk Group	Help Desk Group	HD	private
☐	Human Resources Group	Human Resources Group	HR	private
☐	Marketing Group	Marketing Group	Marketing	private
☐	Sales Group	Sales Group	Sales	private
☐	Support Group	Support Group	Support	private

To update a group definition, click group ID of the group definition that you want to change. When the changes are made, click **Update** to update the definition.

To delete a group definition, select the check box next to the group that you want to delete and click **Delete**. Multiple group definitions can 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 page. Click **Manage Groups**.

Departments

With the **Users** > **Departments** option, you can add and manage departments.

For more information about how departments should be utilized, see Delegated Administration.

Add Department

Click **Users** > **Departments** > **Add Department** to add department definitions on the Add Department page.

Departments can only be added by an administrator who has access to the entire TIBCO 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 Required Department Information, which defines parameters that are required to create a department record.

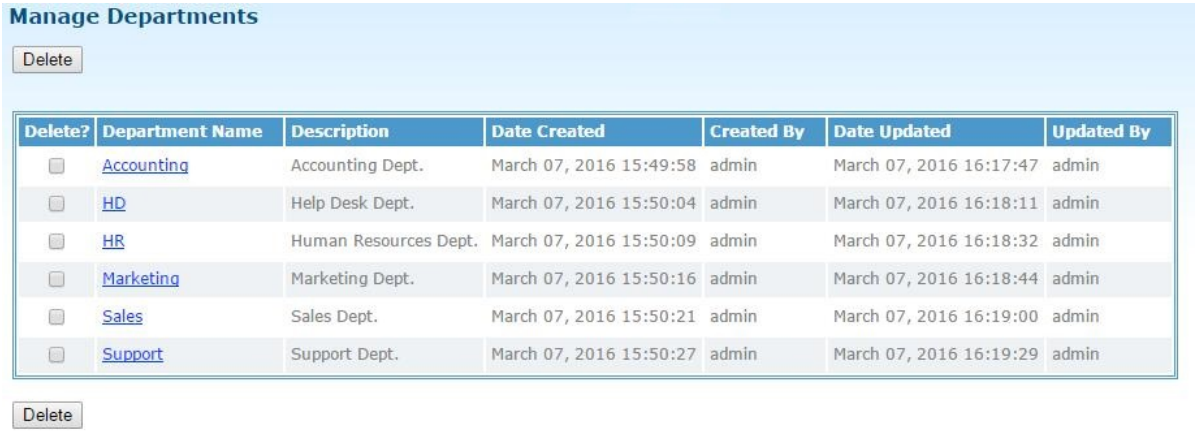
Manage Departments

Click **Users** > **Departments** > **Manage Departments** to manage department definitions on the Manage Departments page.

Administrative users must have AdministratorRight to manage department definitions.

On the Manage Departments page, you can list, update and delete the department definitions.

The following figure shows an example of 6 departments that have been created and can be managed on 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 **List Next 100** to access the next 100 department definitions. You also can click **Back** to see the previous definitions.



To update a department definition, click the department name of the department definition that you want to change. When the changes are made, click **Update** to update the definition.

To delete a department definition, select the check box next to the department that you want to delete and click **Delete**. Multiple department definitions can 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 page. Click **Manage Departments** .

Servers

With the **Servers** option, you can add and manage servers and server credentials.

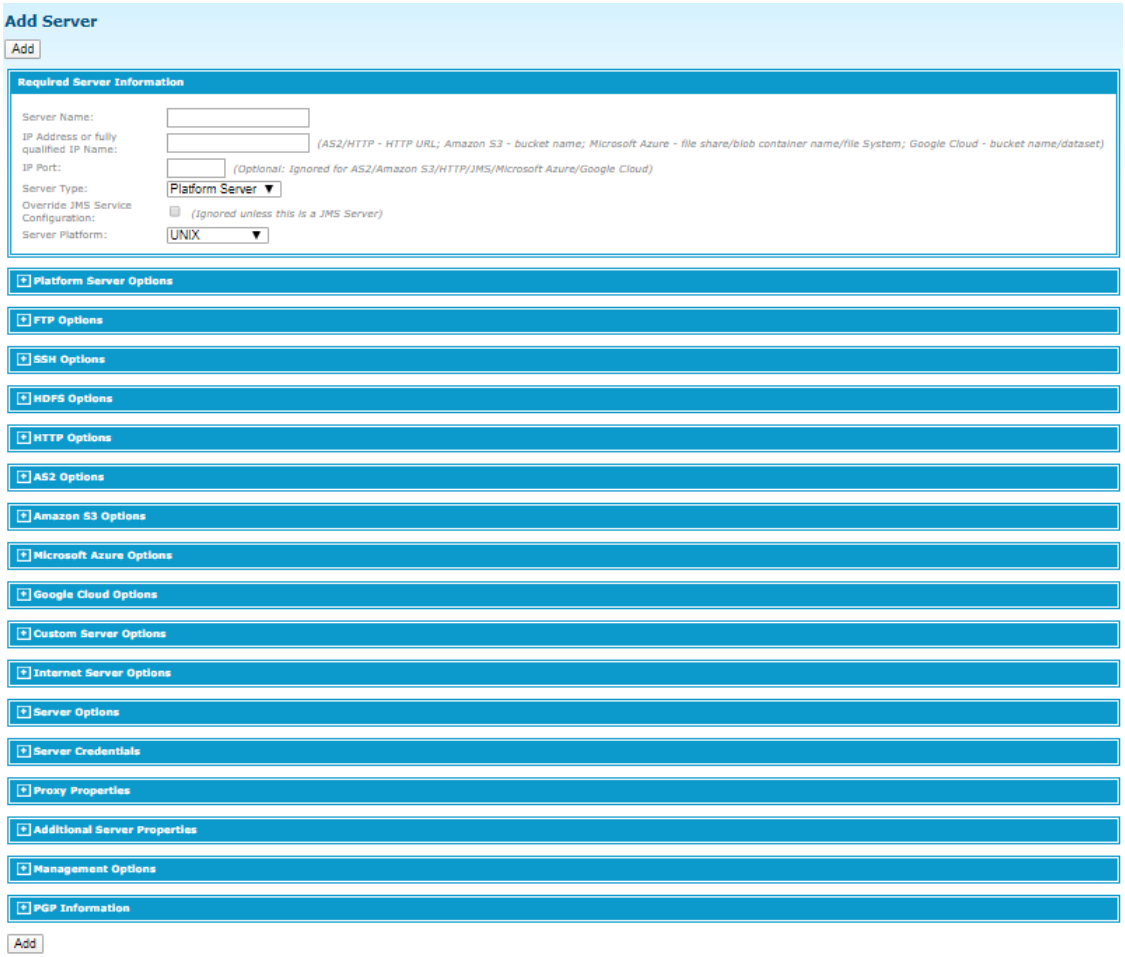
Server definitions contain the information that TIBCO MFT Internet Server needs to communicate with the following server types. The server definition defines how the supported client's can gain access to a file. For more information about how to configure the fields on this page, see the online help page.

Server Type	Description
Platform Server	TIBCO® Managed File Transfer Platform Server for Windows, UNIX, z/OS or IBMi using the CFI protocol with or without SSL.
Internet Server	Used in conjunction with TIBCO ActiveMatrix BusinessWorks™ plug-in and JMS servers.
JMS	Used when sending files to a JMS server or receiving files from a JMS server.  The connectivity information for the JMS server is defined on the Configure JMS Service page in TIBCO MFT Command Center. The IP address and name defined in this definition are ignored.
FTP	Used when remote system is using an FTP/FTPS server.  The FTP/FTPS server on an IBMi operating system is not supported.
Local	Used when writing files to the local TIBCO MFT Internet Server server.
SSH	Used when the remote system is using an SSH server.
AS2	Used when communicating with a remote AS2 server.
HDFS	Used when sending files to or receiving files from remote HDFS (Hadoop Distributed File System) servers.
File Share	Used when MFT clients (FTP, SFTP, HTTP, Platform Server) are sending files to or receiving files from the File Share component of MFT.
HTTP	Used when sending files to or receiving files from remote HTTP servers.
Amazon S3	Used when transferring files to/from Amazon S3 storage.
Microsoft Azure	Used when transferring files to/from Microsoft Azure storage.
Google Cloud	Used when MFT clients (FTP, SFTP, HTTP, Platform Server) are sending files to or receiving files from Google Cloud.
Custom Server	Used when MFT clients (FTP, SFTP, HTTP, Platform Server) are sending files to or receiving files from custom servers.

Add Server

Click **Servers** > **Add Servers** to add remote servers to the TIBCO® Managed File Transfer Platform Server system on the Add Server page.

Administrative userA must have AdministratorRight or UpdateServerRight to add a server.



The Add Server page contains the following sections:

- Required Server Information
- Platform Server Options
- FTP Options
- SSH Options
- HDFS Options
- HTTP Options
- AS2 Options
- Amazon S3 Options
- Microsoft Azure Options
- Google Cloud Options
- Custom Server Options
- Internet Server Options
- Server Options
- Server Credentials
- Proxy Properties
- Additional Server Properties

- Management Options
- PGP Information

Required Server Information

This section defines the parameters that are required to create a server record.

When defining FTP or SFTP servers located on Windows, specify `UNIX` because most FTP and SFTP servers use UNIX format commands. FTP server on IBM iSeries is not supported.

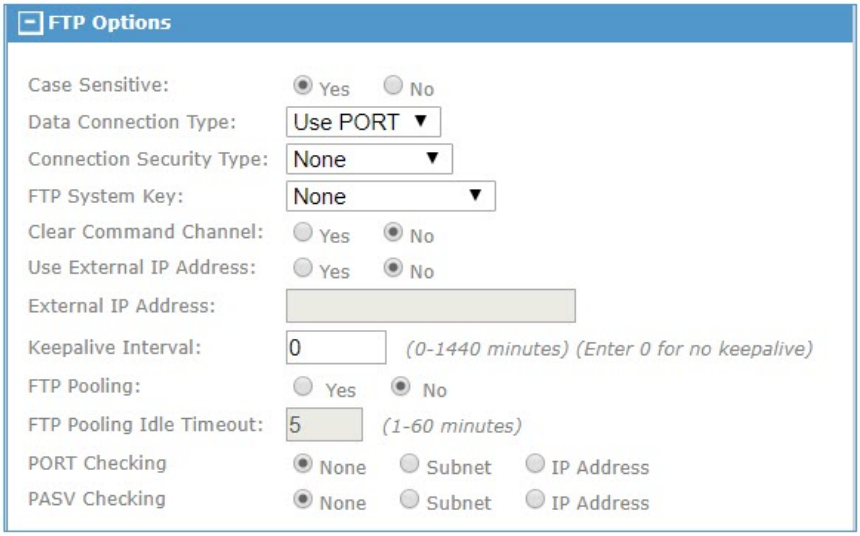
For a JMS Server, if you select the **Override JMS Service Configuration** check box, the URL defined in the **IP Address or fully qualified IP Name** field overrides the URL defined in the Configure JMS Server page. If you do not select the **Override JMS Service Configuration** check box, the URL defined in the Configure JMS Server page is used and the URL defined in the **IP Address or fully qualified IP Name** field is ignored.

Platform Server Options

This section defines server parameters that are used only when the server type is defined as `Platform Server`.

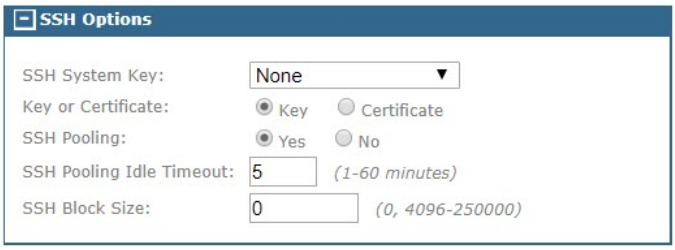
FTP Options

This section defines server parameters that are used only when the server type is defined as `FTP`.



SSH Options

This section 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.



HDFS Options

This section defines server parameters that are used only when the server type is defined as `HDFS`.

HTTP Options

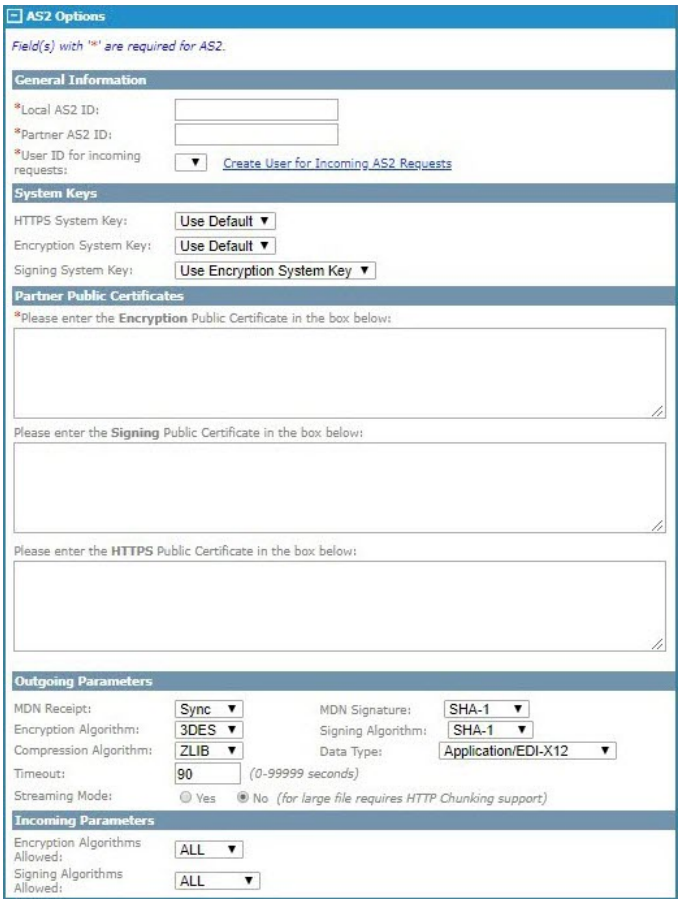
This section defines server parameters that are used only when the server type is defined as `HTTP`.

AS2 Options

This section defines server parameters that are used only when the server type is defined as `AS2`.

Consider the following points when configuring these server options:

- Local AS2 ID should be set to the same local AS2 ID defined on the Configure AS2 Server page.
- 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 TIBCO MFT Internet Server server, no configuration changes are needed as TIBCO MFT Internet Server is configured for HTTP chunking.
- The Checkpoint Restart function is not supported for transfer to/from an AS2 server and should not be enabled in a transfer definition defined for an AS2 server.



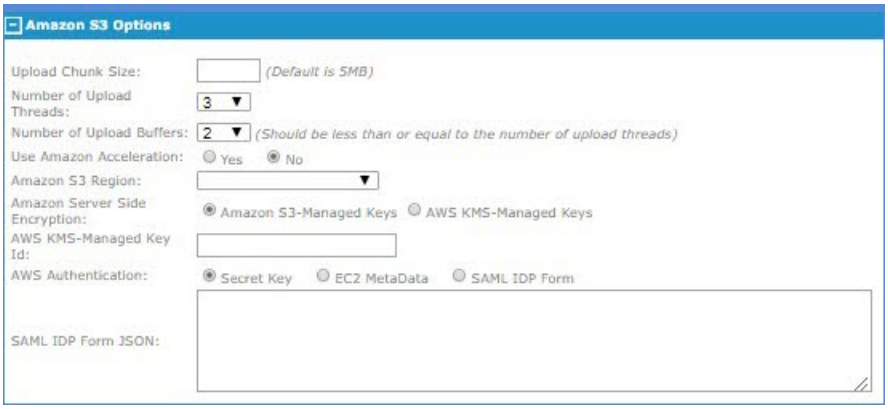
Amazon S3 Options

This section defines the parameters required to access files located on an Amazon S3 Bucket.

Consider the following point when connecting to an Amazon S3 Server:

Setting the **Upload Chunk Size** and **Number of Upload Buffers** too large can cause clients to timeout waiting for MFT to send the buffers. This can happen when the client connection to MFT is faster than the MFT connection to Amazon S3. This can cause re-transmissions of files when no error has occurred, particularly when using FTP or SFTP clients that have a short timeout value.

See the Admin Help pages for detailed information on these parameters.



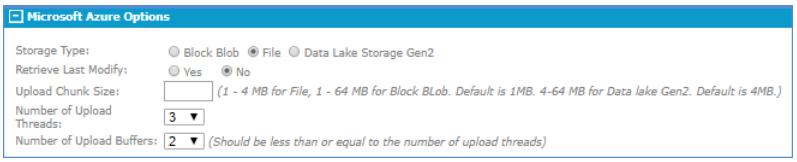
Microsoft Azure Options

This section defines the parameters required to access files, blobs, and Data Lake Storage Gen2 located on Microsoft Azure.

Consider the following point when connecting to a Microsoft Azure Server:

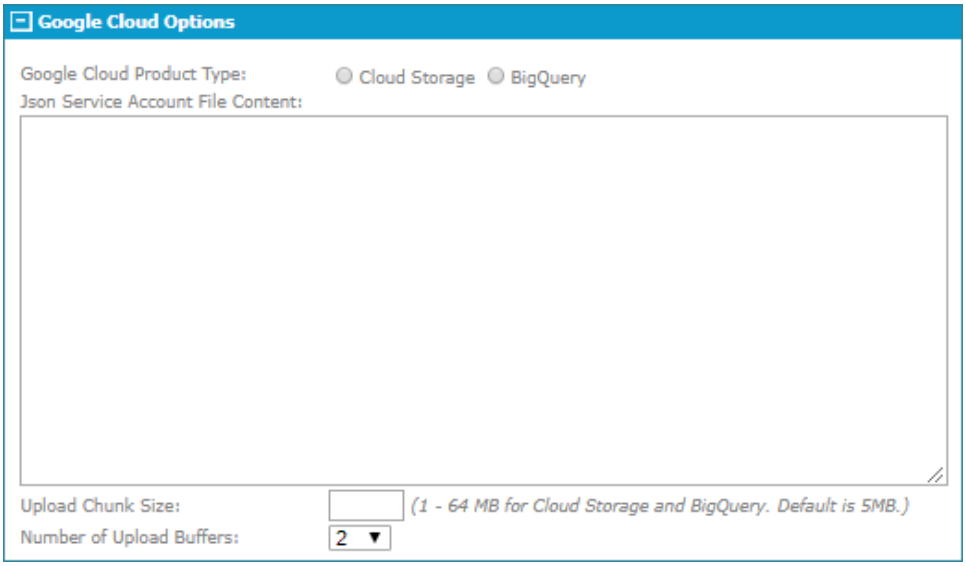
Setting the "Upload Chunk Size" and "Number of Upload Buffers" too large can cause clients to timeout waiting for MFT to send the buffers. This can happen when the client connection to MFT is faster than the MFT connection to Azure. This can cause re-transmissions of files when no error has occurred, particularly when using FTP or SFTP clients that have a short timeout value.

See the Admin Help pages for detailed information on these parameters.



Google Cloud Options

This section defines the parameters that are used only when the server type is defined as `Google Cloud`. These parameters are required to access Cloud Storage and BigQuery. Based on the Google product, enter the Google Storage bucket name for Cloud Storage or the BigQuery dataset name for BigQuery. The **JSON Service Account File** content defines the JSON Service Account Key associated with the service account. This JSON data is used as credentials to access the Google Cloud products. (Credentials in **Server Credentials** are ignored.)



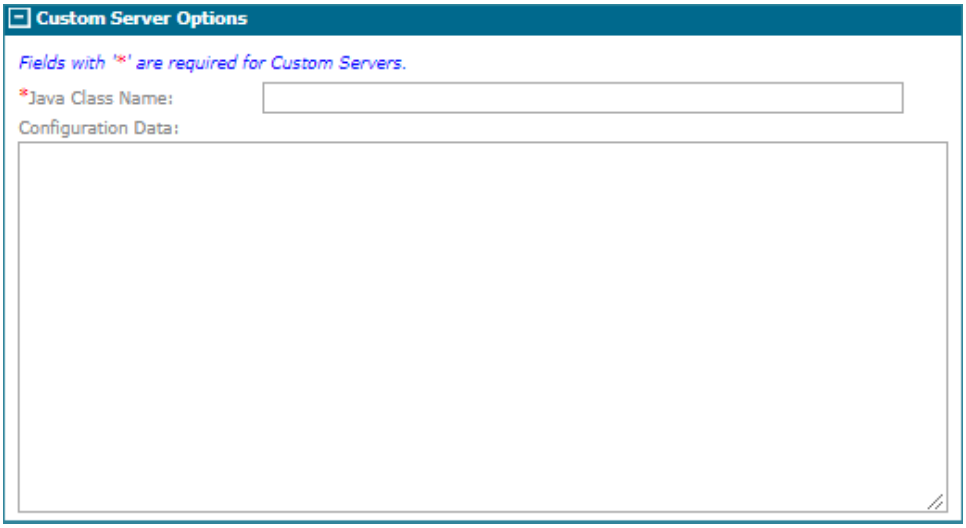
Custom Server Options

This section defines the parameters that are used only when the server type is defined as `Custom Server`. Custom servers allow you to support protocols not supported by MFT. Custom servers provide a Java interface that allows you to integrate custom protocols into the MFT architecture. You must provide the Java class name that defines an implementation of the "com.tibco.mft.transfers.custom.CustomTransfer" interface for the Custom Server.

You can also enter any data that should be passed to the custom interface code. You can pass any text data in the **Configuration Data** field, including, but not limited to, JSON, XML or CSV data. No validation is performed on the data in the **Configuration Data** field, so you must ensure that the data is formatted correctly. Up to 65536 bytes of data are allowed in this field. The Custom Server interface allows you to

enter the following three tokens to pass credentials associated with this server to the custom code. In this way, you do not need to enter clear text passwords into the configuration box.

- $(UserId) - Passes the clear text user ID to the customer interface code.
- $(Password) - Passes the clear text password to the customer interface code.
- $(Domain) - Passes the clear text domain name to the customer interface code.



Internet Server Options

This section defines the Internet Server context that are used only when the server type is defined as `Internet Server`. You must indicate if the port being defined for the server is a secure port or not.

Server Options

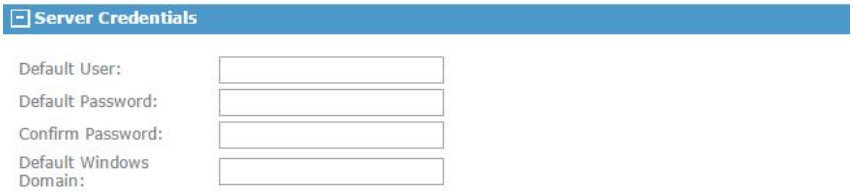
This section is used to predefine a default path that file uploads and downloads would use. This can be very helpful when defining transfer definitions. For example, the path could be defined here and, in the transfer definition, the adminitrator could define file name tokens without defining a path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

Note: This field cannot be overridden.

Server Credentials

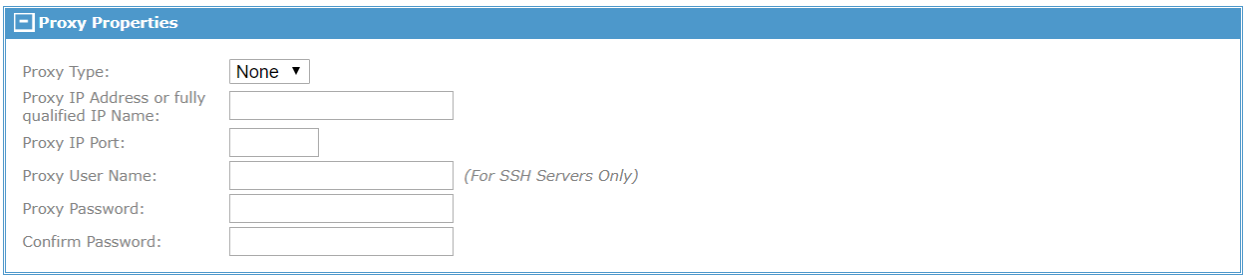
This section defines a default user ID and password to be used for this server. These credentials are used for transfers as well as Platform Server audit collection purposes. See the Collection Service page in TIBCO MFT Command Center for more information about how to collect Platform Server audits.

These credentials can be overridden for transfers from a transfer definition or a Platform Server transfer definition.



Proxy Properties

This section defines parameters specific to the proxy, such as proxy type, address, port, and authentication.



Additional Server Properties

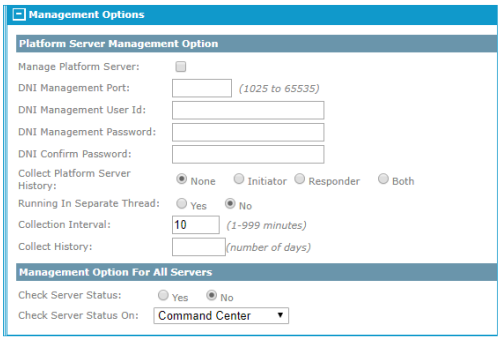
This section defines parameters specific for this server, such as department, description and trace level.

Management Options

This section contains two subsections. The **Check Server Status** area allows TIBCO MFT Command Center 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`. **Check Server Status On** allows you to define the server where the server status request is performed. By default, the server status request is done from the Command Center server where the server status service is executing. If you select an Internet Server from the drop-down box, server status requests for this server are done from the selected Internet Server instance.

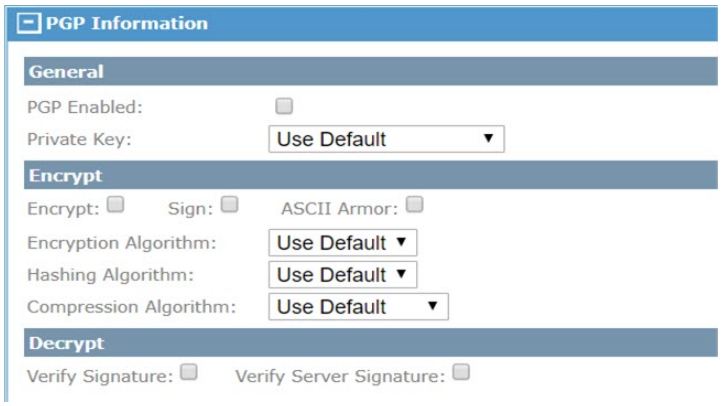
When you want to collect Platform Server audit records, select the **Manage Platform Server** check box. Then, specify the **Collect Platform Server History**, **Collection Interval**, and **Collect History** fields. You will be told you need to restart the collection service, if you have it running already.

For more information about collecting audit logs from Platform Server, see the Collection Service page in TIBCO MFT Command Center. If the administrator will be managing DNI (Directory Named Initiation) from TIBCO MFT Command Center, you must specify the DNI port, DNI user ID, and password. TIBCO MFT Command Center and TIBCO MFT Internet Server both distribute the DNI perl programs, templates and instruction manual within the `dni.tar` file located in the *`MFTIS_Install`*`\distribution\dni` directory. To extract the files from the `dni.tar` file, type `tar -xvf dni.tar` on a command line.



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 TIBCO MFT Command Center or imported into the system by the administrator through the TIBCO MFT Command Center or TIBCO MFT Internet Server administrator web pages or by an end user through the browser client. For more information about the browser client, see the *TIBCO Managed File Transfer Internet File Transfer and File Share Clients User's Guide*.



Manage Servers

Click **Servers** > **Manage Servers** to manage server definitions on the Manage Servers page.

Users must have AdministratorRight or UpdateServerRight to manage server definitions.

You can list, search, and delete TIBCO MFT Internet Server/Internet Server server definitions on this page.

The following figure shows an example list of 5 servers (`*LOCAL` is set by default) that had been added to TIBCO MFT Internet Server. They can be managed on the Manage Servers page. It also gives you the capability to search the server database to limit the number of server definitions displayed. For more information about how to configure the fields on this page, see the online help page.

Selection Criteria

When the **Selection Criteria** section is expanded by clicking the plus sign (+), you will see the available fields a search can be conducted with. This section allows you to selectively search the server record database to limit the number of records that are displayed in the results table. A percent sign (%) 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 **Search** to perform the search and create the results table.

Results Table

The results table will display all the servers you have defined in the system. If you click 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 want to delete and click **Delete**. Multiple server definitions can 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 page. Click **Manage Servers**.

Server Credentials

With the **Servers** > **Server Credentials** option, you can add and manage server credentials.

The user must have AdministratorRight or UpdateServerCredentialRight to manage the server credentials. For more information about how to configure the fields on this page, see the online help page.

Add Server Credentials

Click **Servers** > **Server Credentials** > **Add Server Credentials** to add server credential definitions on the Add Server Credentials page.

The Add Server Credentials page contains the following sections:

- Required Server Credential Information
- Windows Properties

Required Server Credential Information

This section defines the parameters that are required to create a server credential record.

Windows Properties

Server credentials are checked in the following order:

1. User ID
2. Group

If the user is not found in any defined server credentials, the server credentials defined in the server definition will be used.

Upon the login, the remote TIBCO Managed File Transfer (MFT) Platform Server authentication validates that the remote user ID is:

1. Administrator
2. Part of the Local Administrators group
3. Part of the cfadmin or cfbrowse group depending on the action being attempted

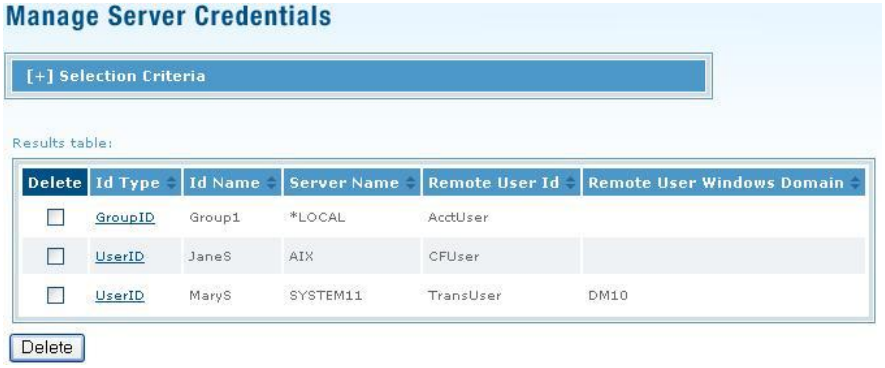
Manage Server Credentials

Click **Servers** > **Server Credentials** > **Manage Server Credentials** to manage server credential definitions on the Manage Server Credentials page.

Users must have AdministratorRight or UpdateServerCredentialRight to manage server credential definitions. For more information about how to configure the fields on this page, see the online help page.

You can list, search, update and delete server credentials definitions on this page.

The following figure shows an example of 3 user credentials that had been added at an earlier date and can be managed on 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 **List Next 100 >** to access the next 100 server credential definitions. You also can click **Back** to see the previous definitions.



A listing of particular server credentials can be obtained by entering the search criteria for any combination of ID type, ID name, node name, remote user ID and remote user Windows domain. A percent sign (%) can be used as a wildcard character.

To update a server definition, click the ID type of the server credential definition that you want to change. When the changes are made, click **Update** to update the definition.

To delete a server credential definition, select the check box next to the server credential that you want to delete and click **Delete**. Multiple server credential definitions can be deleted at one time.

If you want to refresh the **Manage Server Credentials** list, you can use the navigation box on the left portion of the page. Click **Manage Server Credentials**.

Administration

With the **Administration** option, you can configure, manage transfer servers, monitor activities and manage LDAP configurations.

For more information about how to configure the fields on this page, see the online help page.

System Configuration

Click **Administration** > **System Configuration** to specify default values for TIBCO MFT Internet Server.

This page contains the following sections:

- Global Settings
- Password Reset and Self Registration Rules
- Global Password Rules
- Transfer Settings
- Default Settings
- Local Settings
- Remote Settings
- Global Lockout Rules
- Global PGP Settings
- Global FTP Settings
- Global SSH Settings
- Global HTTPS Settings

- Global Platform Settings

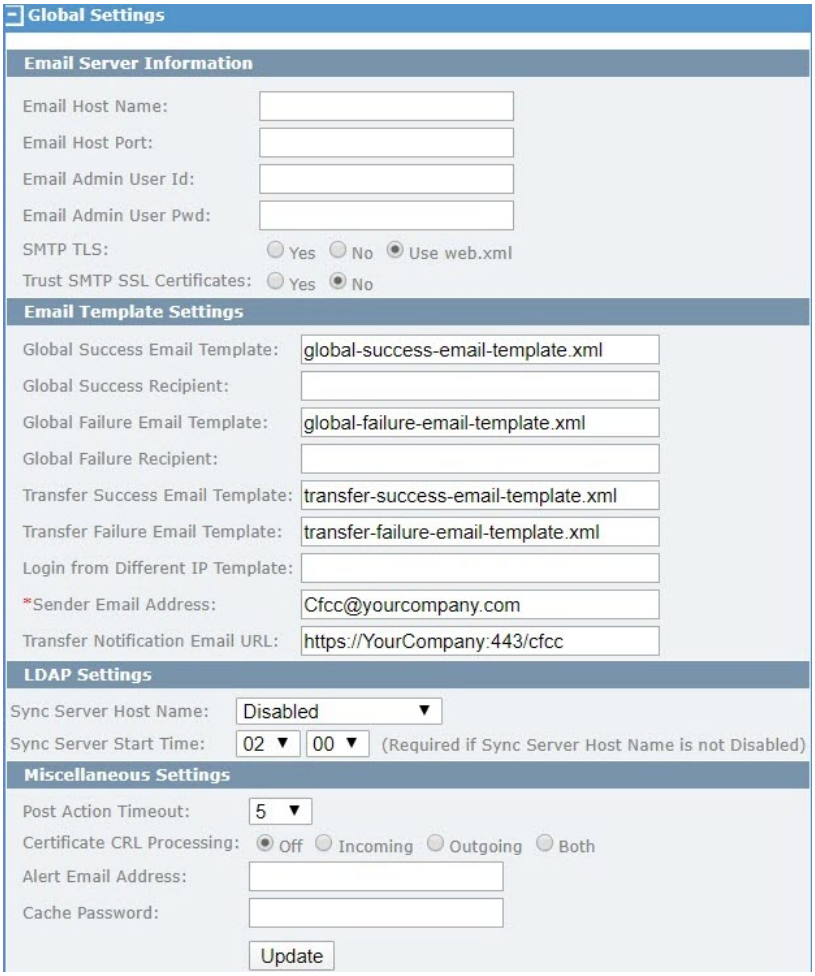
You also can see a Remote Settings section if your environment is configured with multiple Internet Server servers or Internet Server servers pointing to the same database.

For more information about how to configure the fields on this page, see the online help page.

Global Settings

The Global Settings section defines settings common to all TIBCO MFT Internet Server servers.

Global success email and failed transfer notifications do not apply to AS2 transfers.

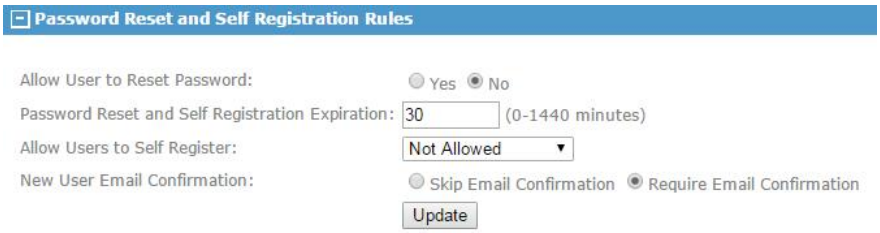


Password Reset and Self Registration Rules

The Password Reset and Self Registration Rules section defines whether to allow users to self register and reset their own passwords.

When an end user requests help accessing their account from the TIBCO MFT Command Center sign-on page and clicks **Reset your password**, they will be prompted to enter and submit their email address associated with their account. The email server information must be configured on the System Configuration page for this feature and an email address defined in the end users account.

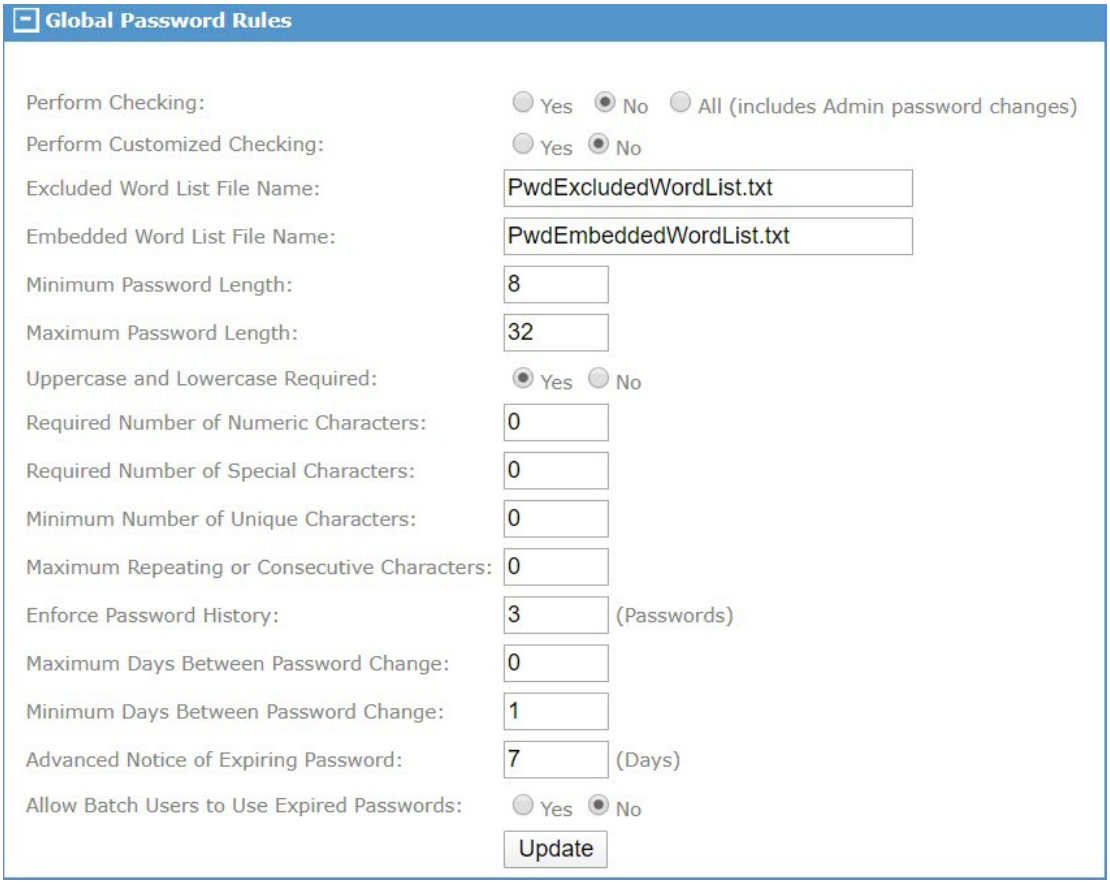
They will receive an email with a link to reset their password. The password requests sent to end users will expire based on the minutes defined in the **Password Reset and Self Registration Expiration** field. The default value is `30`. A value of `0` will result in the password request never expiring. Maximum value allowed is `1440`.



Global Password Rules

The Global Password Rules section defines global rules for changing and expiring passwords.

These password rules would only apply to Internet Server users. Any LDAP sync users' passwords would be controlled by the LDAP server.



Transfer Settings

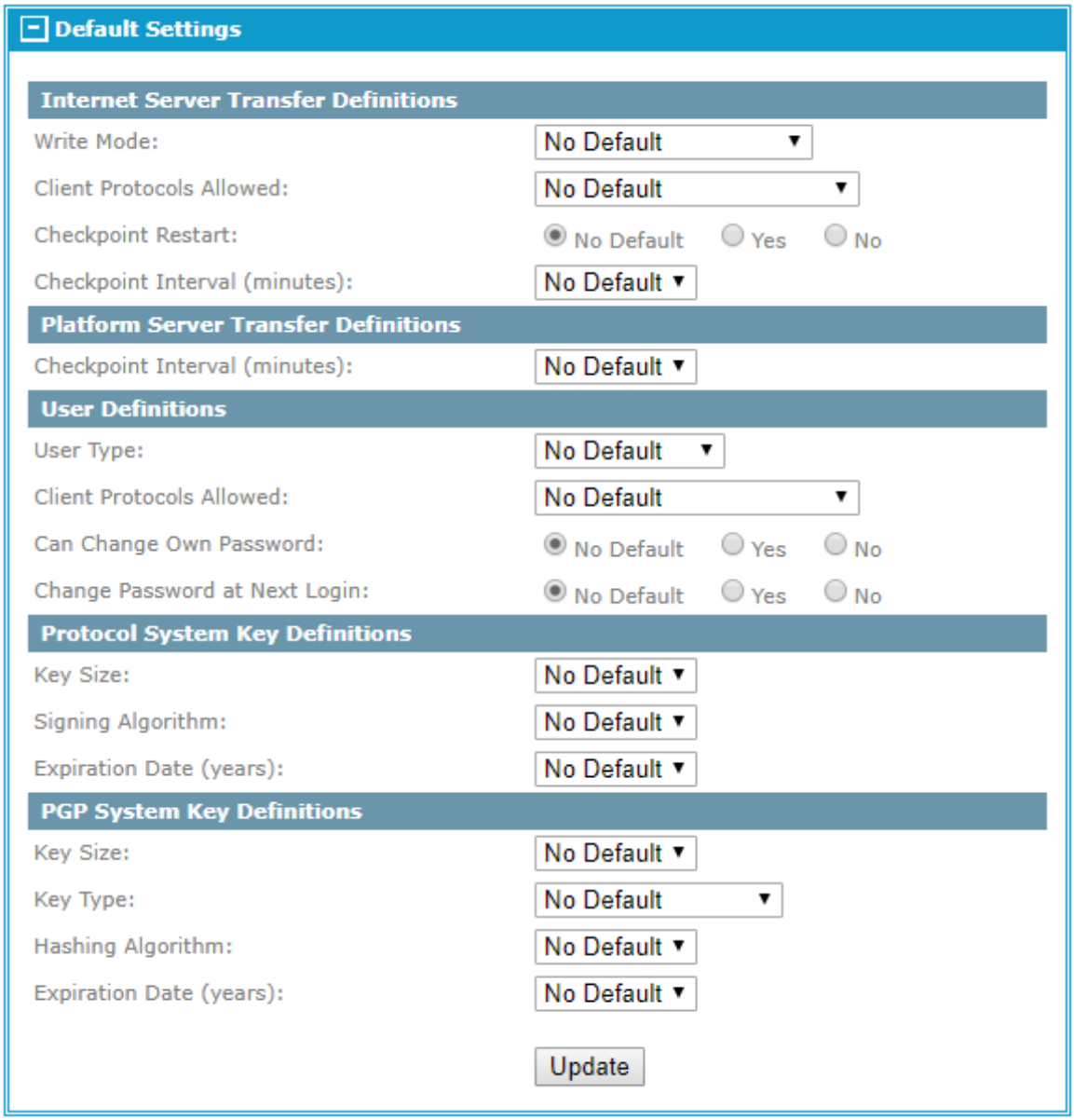
The Transfer Settings section defines the file transfer rules. These rules define the types of files that can be uploaded or downloaded.

Default Settings

You can define the default settings. The Default Settings section allows you to override the default values of parameters in other admin pages.

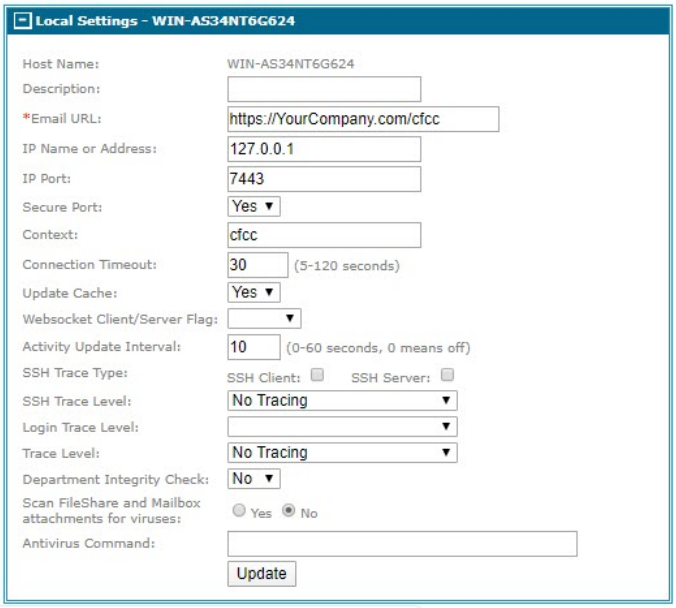
These default settings apply only to settings on the admin pages. They do not apply to settings on SOAP calls, REST calls or the Admin Command Line Interface.

The following figure shows the Default Settings section:


Default Settings
Internet Server Transfer Definitions
Write Mode:
No Default
Client Protocols Allowed:
No Default
Checkpoint Restart:
No Default
Yes
No
Checkpoint Interval (minutes):
No Default
Platform Server Transfer Definitions
Checkpoint Interval (minutes):
No Default
User Definitions
User Type:
No Default
Client Protocols Allowed:
No Default
Can Change Own Password:
No Default
Yes
No
Change Password at Next Login:
No Default
Yes
No
Protocol System Key Definitions
Key Size:
No Default
Signing Algorithm:
No Default
Expiration Date (years):
No Default
PGP System Key Definitions
Key Size:
No Default
Key Type:
No Default
Hashing Algorithm:
No Default
Expiration Date (years):
No Default
Update

Local Settings

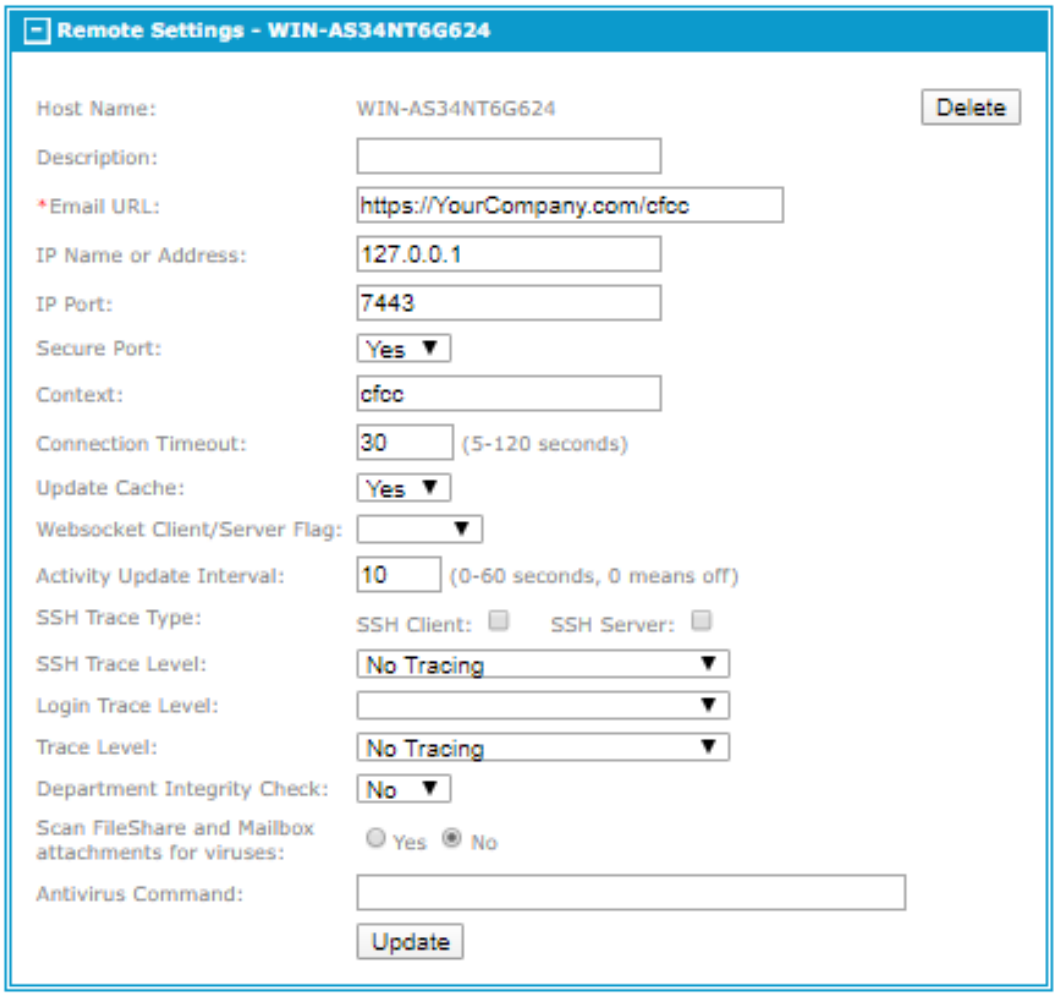
The Local Settings section defines unique settings for the individual TIBCO MFT Internet Server servers that are defined during the installation.



Remote Settings

You can define the settings for other server instances. One box is displayed for each remote server instance. The fields are the same as the fields in the Local Settings section.

The following figure shows the Remote Settings section:

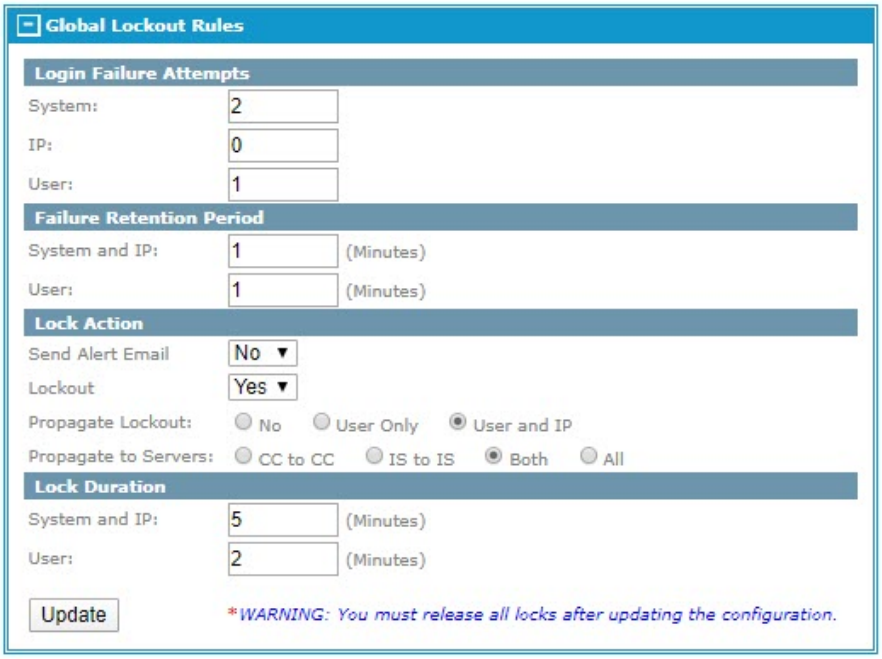


Global Lockout Rules

The Global Lockout Rules section defines global lockout rules that 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`.

The Send Alert Email lock action requires you to configure the **Alert Email Address** field, which is in the Global Settings section on the System Configuration page.



The Failure Retention Period section is reset upon a successful login for user accounts. For example, if the login failure attempts for a user is set to 3 and a user fails to login twice but on the third attempt is successful, the failed attempts will be reset to 0. This also occurs 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 0. 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 administrator 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 for more details about releasing lock outs.

You can define the lock action to be taken when the login failure attempts thresholds are reached within the failure retention period. An alert email is sent to the email address defined in the **Alert Email Address** field of the Global Settings section. The **Lockout** field defines whether lockout processing is to be performed.

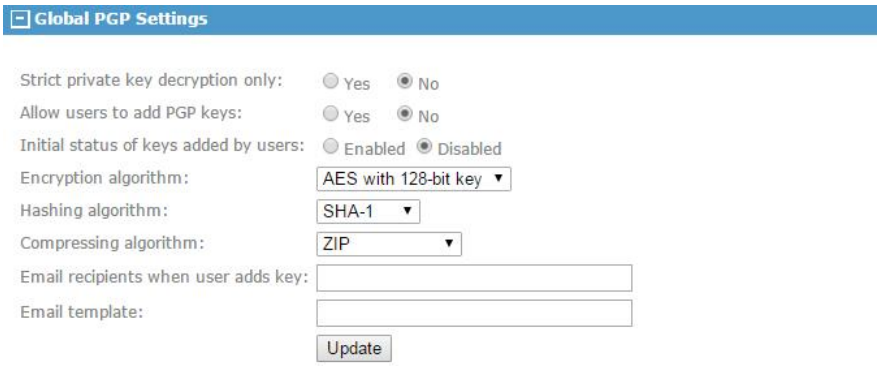
The **Lockout** field must be set to `Yes` when any one value in the Login Failure Attempts section is set to a non-zero value.

The amount of time that a user, IP address, or system is locked out depends on the Lock Duration settings. You can also define whether to propagate lockout between MFT instances and also define the server instances where lockouts are propagated.

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. (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.

Global PGP Settings

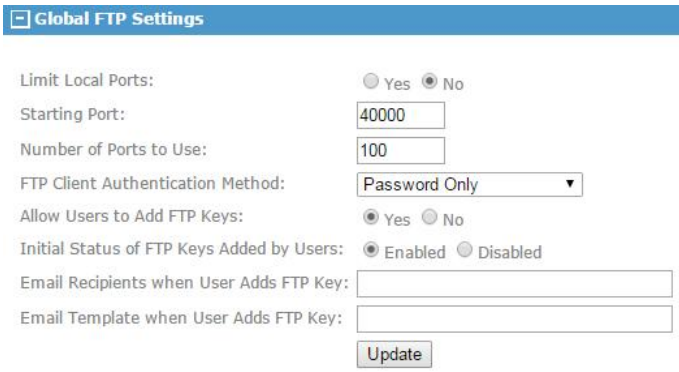
The Global PGP Settings section defines the global PGP settings that will be used by MFT server.



Global FTP Settings

The Global FTP Settings section defines the global FTP settings that will be used by MFT server.

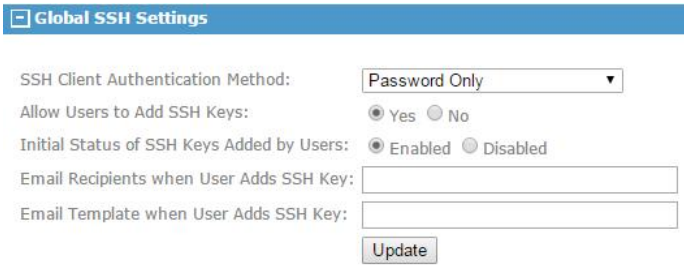
The **FTP Client Authentication Method** field can be overridden by the same field in the Authentication Options section of a user definition.



Global SSH Settings

The Global SSH Settings section defines the global SSH settings that will be used by MFT server.

The **SSH Client Authentication Method** field can be overridden by the same field in the Authentication Options section of a user definition.



Global HTTPS Settings

The Global HTTPS Settings section defines the global HTTPS settings that will be used by MFT server.

The **HTTPS Client Authentication Method** field can be overridden by the same field in the Authentication Options section of a user definition.

Global Platform Settings

The Global Platform Settings section defines the global platform settings that will be used by Internet Server to authenticate Platform Server clients.

File Share

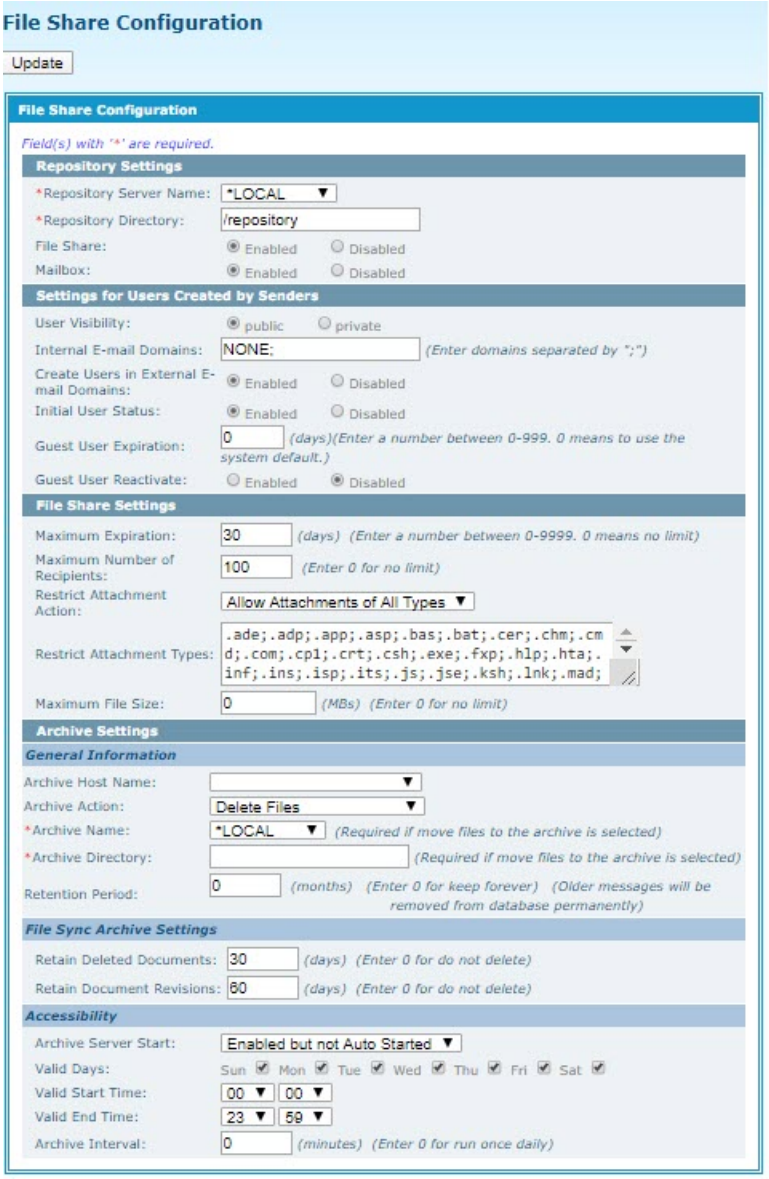
With the **Administration** > **File Share** option, you can configure the File Share server, and start or stop the File Share Archive server.

File Share Configuration

Click **Administration** > **File Share** > **Configuration** to configure the File Share server on the File Share Configuration page.

The File Share Configuration page only has one section named File Share Configuration. This section contains the following subsections:

- Repository Settings
- Settings for Users Created by Senders
- File Share Settings
- Archive Settings



Repository Settings

This section defines the required parameters that define where File Share attachment are stored.

The admin has the ability to enable or disable the file share and mailbox capability. The default value for **File Share** and **Mailbox** fields is **Enabled**.

Settings for Users Created by Senders

This section defines default parameters for users created by File Share senders.

File Share Settings

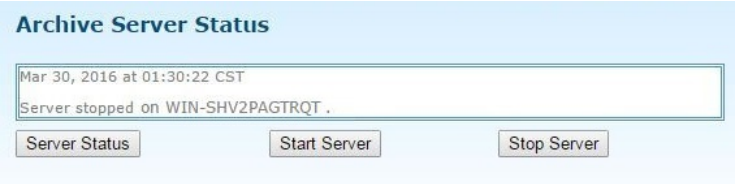
This sections defines default settings and limitations for File Share requests.

Archive Settings

This section defines settings used by the File Share Archive server. The Archive Server cleans up deleted files and files that can be deleted. These settings are grouped into three areas: General Information, Sync Archive Settings and Accessibility.

Archive Server Status

Click **Administration** > **File Share** > **Archive Server Status** to start or stop the File Share Archive server, and check the status of the File Share Archive server on the Archive Server Status page.



Transfer Servers

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

AS2 Server

With the **Administration** > **Transfer Servers** > **AS2 Server** option, you can configure, start, stop and check the status of the AS2 server.

The administrative user must have the Administrator right to configure and start or stop the AS2 server. For more information about how to configure the fields on this page, see the online help page.

AS2 Server Status

Click **Administration** > **Transfer Servers** > **AS2 Server** > **AS2 Server Status** to start or stop the AS2 server and check the status of the server.

Configure AS2 Server

Click **Administration** > **Transfer Servers** > **AS2 Server** > **Configure AS2 Server** to configure the AS2 server on the Configure AS2 Server page.

Before the AS2 server can be started, it must first be enabled and configured.

Firstly, select **Yes** from the **Enabled** list.

Next, specify both the **Receive URL** and **Async Response URL** fields. Both URL's are created from information taken during the installation of TIBCO MFT Internet Server and need to be specified with the correct HTTP protocol information and port.

Then, 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 can be skipped.

You can also define a local AS2 server ID in the server definition that would be used for incoming transfer being done with the TIBCO MFT Internet Server AS2 server or you can leave this field blank and specify it in later when creating a server definition. If this field is configured, it can also be overridden in the server definition.

Finally, click **Update** when your changes are completed.

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 Internet Server defined for this box only.

TIBCO Accelerator

TIBCO Accelerator allows you to greatly improve data transfer speeds over IP networks with high latency.

Tests have shown transfers completing up to 10 to 100 times faster overcoming the slowness due to latency problems. We have added the TIBCO Accelerator file transfer technology to TIBCO MFT Internet Server to provide enterprises with a faster way to send files to business partners or divisions abroad where there are normally latency problems in long distance connections.

TIBCO Accelerator uses its own variation of User Datagram Protocol (UDP) and the TIBCO Accelerator's parallel implementation of TCP, called Parallel Delivery Protocol (PDP).

When TIBCO Accelerator is running, it acts as a responder to transfer requests initiated by our TIBCO MFT Internet Server desktop client ClickOnce application. For more information about the TIBCO MFT Internet Server desktop client, see Appendix E in *TIBCO Managed File Transfer Internet Server Installation Guide*.

To use TIBCO Accelerator, you will need to install Microsoft Visual C++ 2008 Redistributable on the machine where TIBCO MFT Internet Server desktop client is installed. The installation file is distributed with the TIBCO MFT Internet Server desktop client installation files. For more information, see *TIBCO Managed File Transfer Internet Server Desktop Client User's Guide*.

Manage TIBCO Accelerator

Click **Administration** > **Transfer Servers** > **TIBCO Accelerator** to start or stop TIBCO Accelerator and check the status of TIBCO Accelerator on the Manage TIBCO Accelerator page.

By default, TIBCO Accelerator is listening on port 9000 for requests coming in using the TCP or UDP protocol and listening on port 9002 for requests coming in using the PDP protocol.

When the request has been received, TIBCO Accelerator will then set a port number to be used for the data transmission between the TIBCO MFT Internet Server desktop client and TIBCO MFT Internet Server from the port range 9100 – 9199. When the PDP protocol is used, each transfer selects a port and will open 8 connections on that port.

Ports 9000, 9002 and 9100-9199 would have to be opened in the firewall to allow TIBCO Accelerator client to access TIBCO Accelerator server. If requests are initiated from an external computer, these ports must be opened on the firewall for incoming traffic. If requests are initiated from an internal computer, these ports must be opened on the firewall for outgoing traffic.

FTP Server

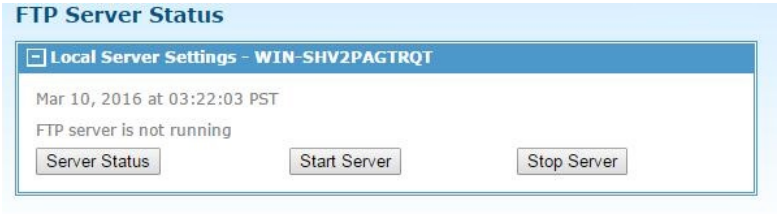
With the **Administration** > **Transfer Servers** > **FTP Server** option, you can configure, start, stop and check the status of the FTP server.

TIBCO MFT Internet Server is set up 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 AdministratorRight to configure and start or stop the FTP server.

FTP Server Status

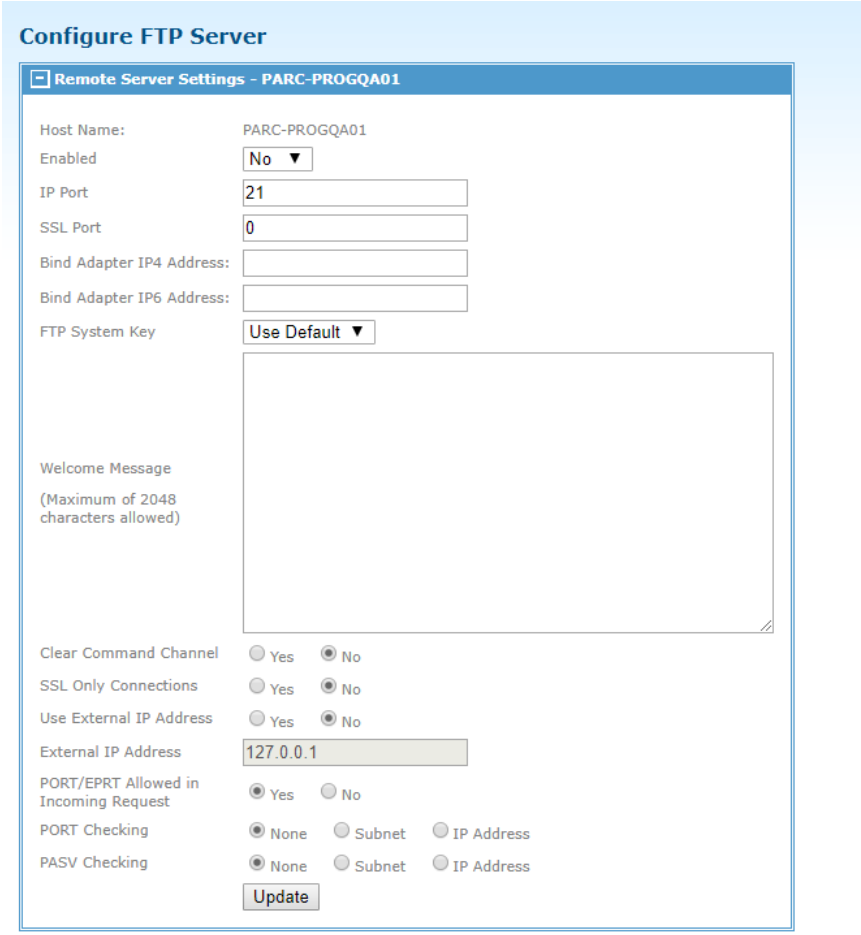
Click **Administration** > **Transfer Servers** > **FTP Server** > **FTP Server Status** to start or stop the FTP server and check the status of the server.

The FTP Server Status page shows 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.



Configure FTP Server

Click **Administration** > **Transfer Servers** > **FTP Server** > **Configure FTP Server** to configure the FTP server on the Configure FTP Server page.



The FTP server is disabled by default, so the server must be enabled before it can be started. When the server is configured, click **Update** to save the settings.

Any fields updated on the page will require the FTP service to be restarted. For more information about how to start and stop the service, See FTP Server Status. For more information about how to configure the fields on this page, see the online help page.

Consider the following points when configuring the FTP server:

- There will be a configurable section for each Internet Server that shares the database. Within each section, there is an **Update** button. When you click this button, the definition changes for Internet Server defined for this box only.
- It is a good practice to specify the **Use External IP Address** area correctly because the IP address defined on some UNIX systems defaults to `127.0.0.1`.
- By default, TIBCO MFT Command Center will request a TLS connection; however if the client does not support TLS, an SSL 3.0 connection can be negotiated. If your environment requires TLS connections, you must use a FIPS approved Java and put your TIBCO MFT Command Center instance in FIPS mode.

Platform Server

With the **Administration** > **Transfer Servers** > **Platform Server** option, you can configure, start, stop and check the status of Platform Server.

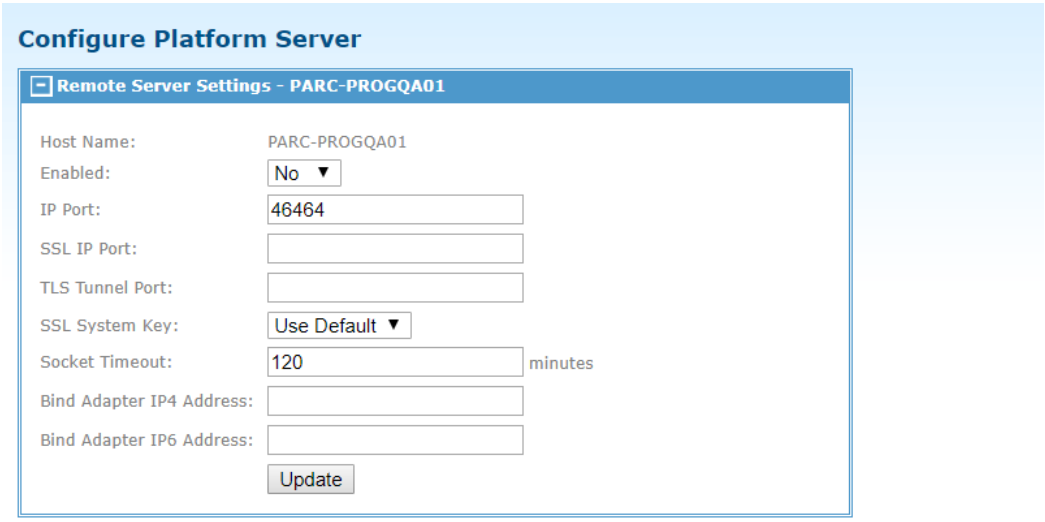
Platform Server allows clients running TIBCO MFT Platform Server on various platforms to send and receive files directly to MFT. Administrative users must have AdministratorRight or FTAdminRight to configure, start or stop the platform server.

Platform Server Status

Click **Administration** > **Transfer Servers** > **Platform Server** > **Platform Server Status** to start or stop Platform Server and check the status of the server.

Configure Platform Server

Click **Administration** > **Transfer Servers** > **Platform Server** > **Configure Platform Server** to configure Platform Server on the Configure Platform Server page.



Platform Server is not enabled by default, so the server must be enabled before it can be started. The administrator would navigate to the Configure Platform Server page, and select **Yes** from the **Enabled** list and either keep or edit the default port of `46464`.

There will be a configurable section for each TIBCO MFT Internet Server server that is in the environment. Within each section, there is an **Update** button. When you click this button, the definition changes for this Platform Server only. When this is complete you would navigate to the Platform Server Status page and start each Platform Server you have configured. For more information about how to configure the fields on this page, see the online help page.

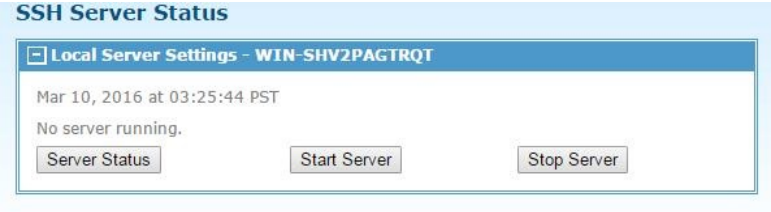
SSH Server

With the **Administration** > **Transfer Servers** > **SSH Server** option, you can configure, start, stop and check the status of the SSH server.

Administrative users must have AdministratorRight to configure and start or stop the SSH server.

SSH Server Status

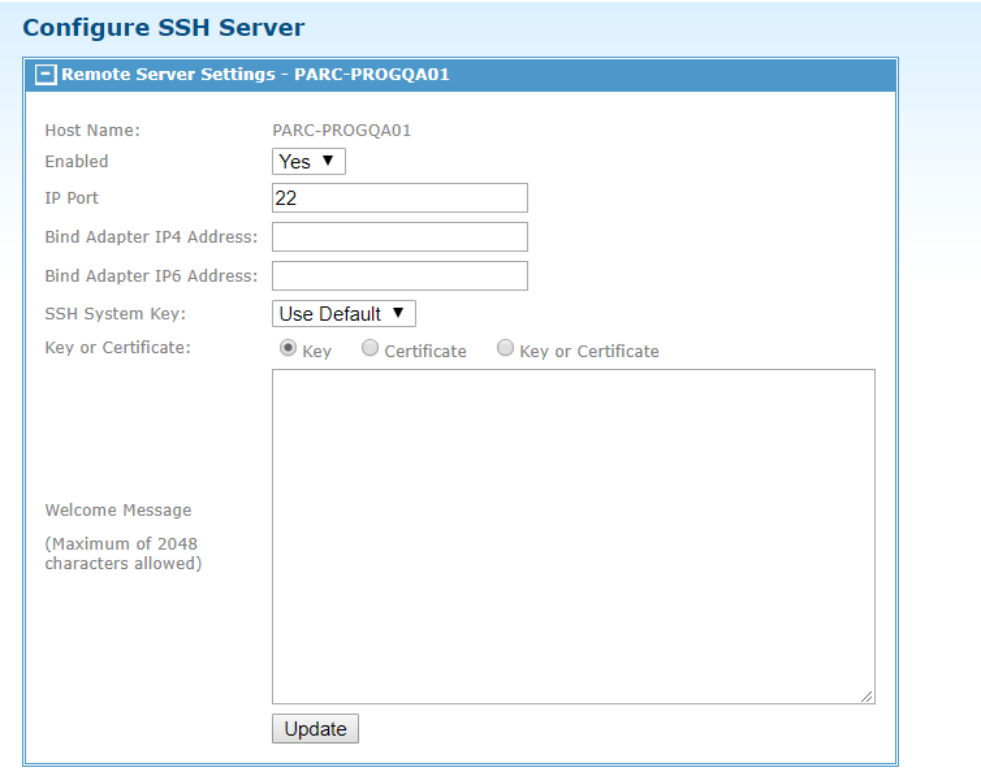
Administration > **Transfer Servers** > **SSH Server** > **SSH Server Status** to start or stop the SSH server and check the status of the server.



There is a section for each defined Internet Server as well as allow the administrator to stop and start the SSH servers. These sections contain the status information about the SSH server on that Internet Server.

Configure SSH Server

Click **Administration** > **Transfer Servers** > **SSH Server** > **Configure SSH Server** to configure the FTP server on the Configure SSH Server page.



Before the SSH server can be started, it must first be configured and enabled. There will be a configurable section for each Internet Server that has been defined. Within each section, there is an **Update** button. When you click this button, the definition changes for 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 you have to select **Yes** from the **Enabled** list. You

should only update the keystore if you want to create a keystore specifically for your installation. For more information about how to configure the fields on this page, see the online help page.

Note: Any changes to the **Welcome Message** field will require the SSH server to be restarted. See SSH Server Status for details.

Protocol Keys

TIBCO MFT Internet Server can create and store AS2, FTP, SSH, Platform Server, and SAML system keys and Kerberos KeyTab files to be used for secure file transfer that are stored in the database.

Administrative users must be super administrators to add or manage any of the TIBCO MFT Internet Server keys. A super administrators has the AdministratorRight right and not a member of a department.

Add Public Key

Click **Administration** > **Protocol Keys** > **Public Keys** > **Add Public Key** to add public keys on the Add Public Key page.

To add a public key that has been received by a 3rd party, select the the type of key that is to be assigned to a server or user from the **Public Key Type** list. Next, choose if the key will be enabled or disabled upon it being added to the database. Then, paste the base64 format of the key into the public key field. Finally, click **Continue**, and then, verify the details to complete saving the public key.

A public key should be in one of the following format:

```
SSH Public Keys
---- BEGIN SSH2 PUBLIC KEY ----
......ssh key information.....
......ssh key information.....
---- END SSH2 PUBLIC KEY ----
```

Or,

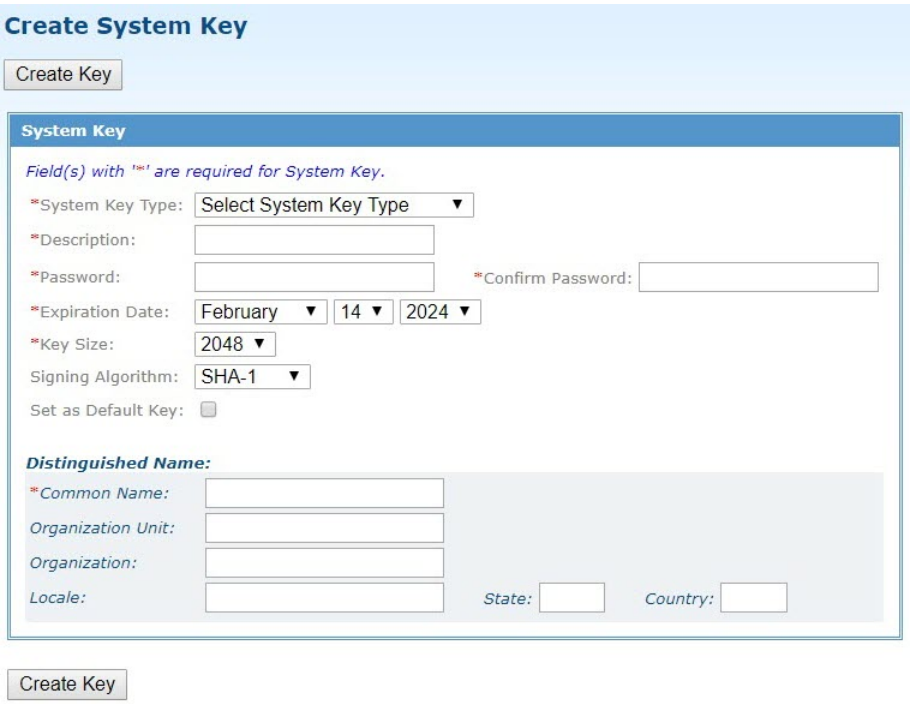
```
ssh-rsa ......ssh key information.....
......ssh key information.....
......ssh key information.....
user@domain
```

Platform, HTTPS and FTPS Public Keys

```
-----BEGIN CERTIFICATE-----
......certificate information.....
......certificate information.....
-----END CERTIFICATE-----
```

Create System Key

Click **Administration** > **Protocol Keys** > **System Keys** > **Create Key** to create system keys on the Create System Key page.



To create a system key, select a system key type that needs to be created. Then, specify the required information and the optional fields as needed and click **Create Key**.

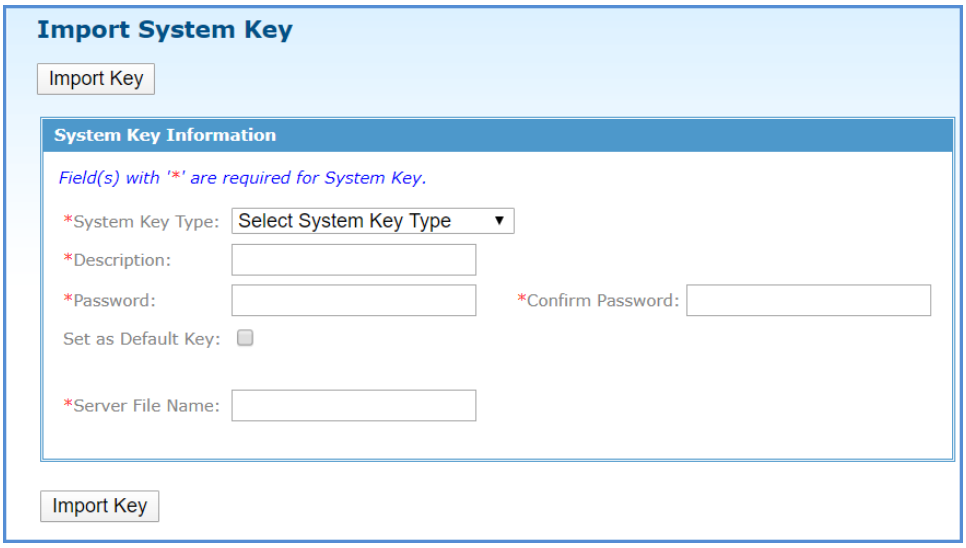
Some servers will not start until a system key is generated for that protocol. For example, the SSH server.

When system key type is `SSH`, the signing algorithm defaults to `SHA-256`.

Import System Key

You can import AS2, FTP, Platform Server, SSH, HTTPS, and SAML system keys through the Import System Key page which can be accessed by clicking **Administration** > **Protocol Keys** > **System Keys** > **Iport Key**.

The following figure shows the Import System Key page:



To import a system key, select a system key type, input the rest of the required information and click **Import Key**.

When importing an SSH, FTPS, Platform Server, HTTPS or SAML key, the jks file defined by the "JKS File Name" parameter must contain only one System Key.

Kerberos Keytab Files

With the **Administration** > **Protocol Keys** > **Kerberos Keytab Files** option, you can import and manage the Kerberos KeyTab files.

The Kerberos KeyTab file is required for the HDFS server with the Kerberos authentication.

Import KeyTab

Click **Administration** > **Protocol Keys** > **Kerberos KeyTab** > **Import KeyTab** to import the Kerberos KeyTab files on the Import KeyTab page.

To import a Kerberos KeyTab file, you need to enter the file path in the **Keytab File Path** field, and provide a description.

By default, the imported file is enabled. If you do not want, clear the **Enabled** check box.

You can also select the **Set as Default Key** check box to set a KeyTab file as the default file for all HDFS servers.

Click **Import Key** after completing the configuration. After TIBCO MFT Internet Server has validated the KeyTab file, click **Confirm**.

The KeyTab file to be imported must be accessible from the MFT server that is importing the KeyTab file.

Manage KeyTabs

Click **Administration** > **Protocol Keys** > **Kerberos Keytab Files** > **Manage KeyTabs** to manage the Kerberos KeyTab files on the Manage KeyTabs page.

This page shows all KeyTab files that have been defined to TIBCO MFT Internet Server.

In the Selection Criteria section, you can search the particular KeyTab files based on the description.

You can delete KeyTab files by selecting the check box next to the KeyTab file that you want to delete and clicking **Delete**. They will be asked to confirm the deletion.

When you click the description of a KeyTab file, you can see the detailed information about that KeyTab file.

Trusted Certificates

With the **Administration** > **Protocol Keys** > **Trusted Certificates** option, you can add and manage 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 trusted certificates to TIBCO MFT Internet Server. When certificate authentication is enabled for your SSH server through the **Administration** > **Transfer Servers** > **SSH Server** > **Configure SSH Server** option 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 distinguished name defined in the user definition to associate the certificate with a user.

If you want to monitor a CRL (Certificate Revoke List) for revoked certificates. You would need to save the CRL list in the *<MFTIS_Install>**<context>*\ftp\crl directory. Then, navigate to **Administration** > **System Configuration** page and expand the Global Settings section. Here, you would set the **Certificate CRL Processing** area. All outgoing CRL processing is for server certificate authentication. Incoming processing is for either the user or server authentication.

For the incoming processing, if a certificate is assigned to a user or server, the trusted certificate is not checked. In addition, TIBCO MFT Internet Server checks the following items:

- If the certificate is enabled.
- If the certificate CRL processing is enabled.

If no certificate is found assigned to a user or server, the trusted certificates will be used for validation, performing the following tasks:

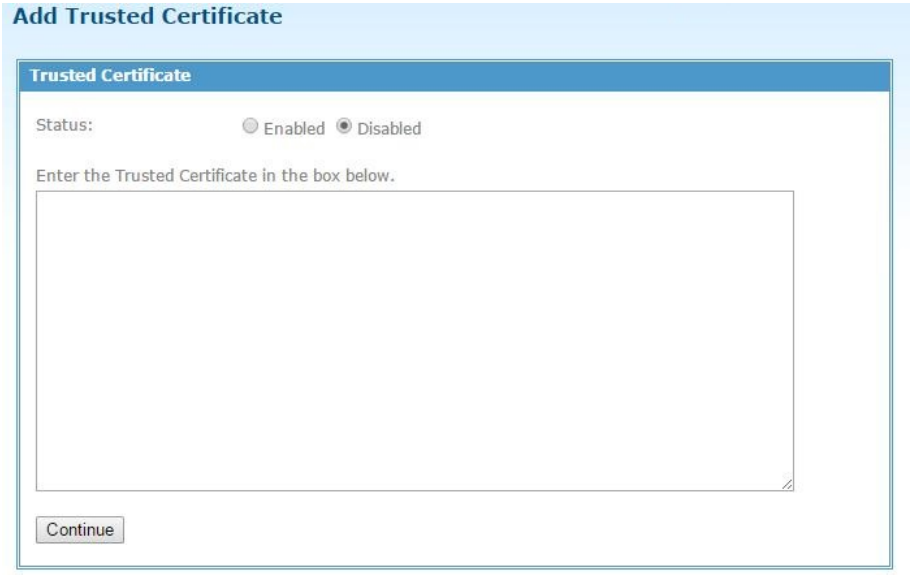
1. Verify the certificate is signed by one of the trusted certificates in the TIBCO MFT Command Center database.
2. Check the CRL if the certificate CRL processing is enabled.
3. Validate the distinguished name extracted from the certificate against the certificate distinguished name field defined in the user definition.

Add Trusted Certificate

Click **Administration** > **Protocol Keys** > **Trusted Certificates** > **Add Trusted Certificate** to add trusted certificates on the Add Trusted Certificate page.

After you have specified all the fields, click **Continue**. The Add Trusted Certificate Confirmation window is displayed. Click **Continue** to add the certificate.

When 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 definition and provide the certificate distinguish name for that user.



Manage Trusted Certificates

Click **Administration** > **Protocol Keys** > **Trusted Certificates** > **Manage Trusted Certificates** to manage trusted certificates on the Manage Trusted Certificates page.

This page shows the trusted certificates available.

You can delete certificates by selecting the check box next to the certificate that you want to delete and clicking **Delete**. They will be asked to confirm the deletion.

When you click the type of a certificate Type of a certificate, you can see the detailed information about that certificate. On the details page, a certificate can be disabled/enabled and displayed by expanding the Display Trusted Certificate section.

PGP Keys

The PGP public keys are associated with an MFT user or server definition.

Super administrators can add and manage PGP public keys.

PGP Public Keys

With the **Administration** > **PGP Keys** > **PGP Public Keys** option, you can add and manage PGP public keys.

Add PGP Public Key

Click **Administration** > **PGP Keys** > **PGP Public Keys** > **Add PGP Key** to add PGP public keys on the Add PGP Public Key page.

When you have specified all the fields, click **Continue** to add the public key.

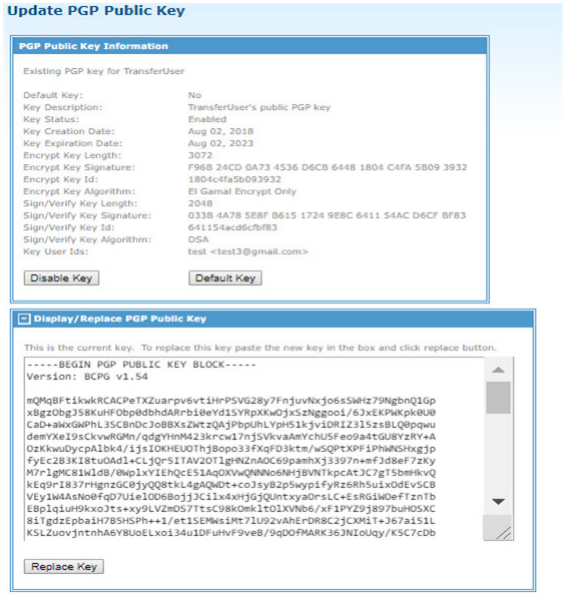
You cannot add a public key for a user or server that already has a public key associated with it. Use the Manage PGP Public Keys page to update or replace a key for a user or server.

Manage PGP Public Keys

Click **Administration** > **PGP Keys** > **PGP Public Keys** > **Manage PGP Keys** to manage PGP public keys on the Manage PGP Public Keys page.

This page shows the PGP public keys available. You can delete keys by selecting the check box next to the key that you want to delete and clicking **Delete**. Then, confirm the deletion.

By clicking on the key type of a particular key, you can see the detailed information about the key. The following figure shows the information that is displayed as a result of clicking **User** for the tuser001 key from the above figure:



PGP System Keys

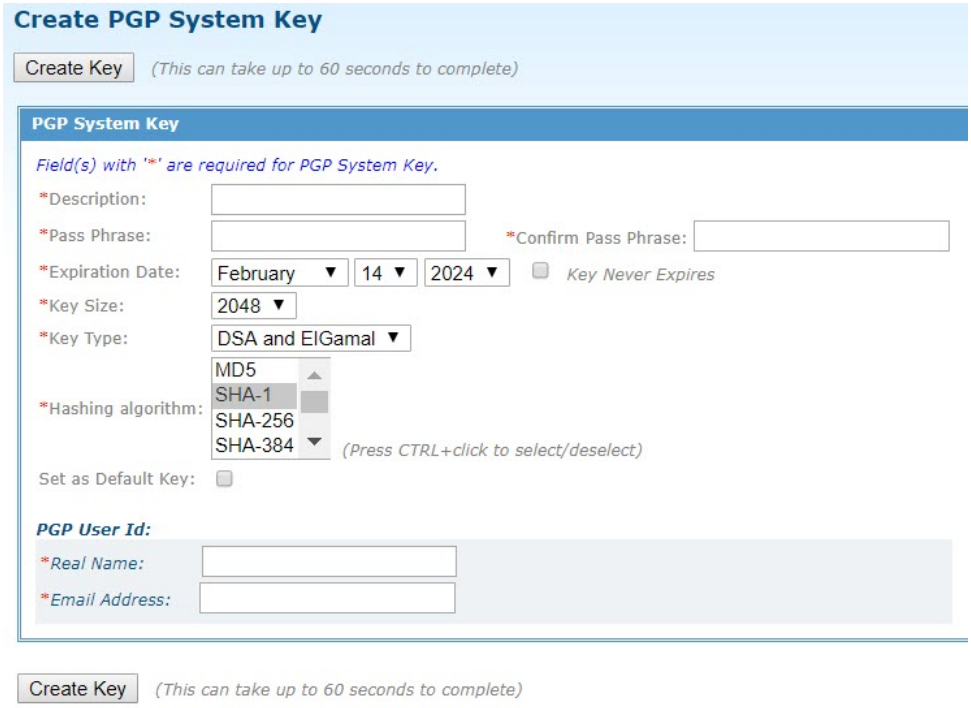
With the **Administration** > **PGP Keys** > **PGP System Keys** option, you can add and manage PGP system keys.

Super administrators can generate PGP keys or PGP keys generated by a PGP or GPG utility can be imported into the MFT database. Please see the Help screen for more information on generating keys.

Create PGP System Key

Click **Administration** > **PGP Keys** > **PGP System Keys** > **Create PGP Key** to add PGP system keys on the Create PGP System Key page.

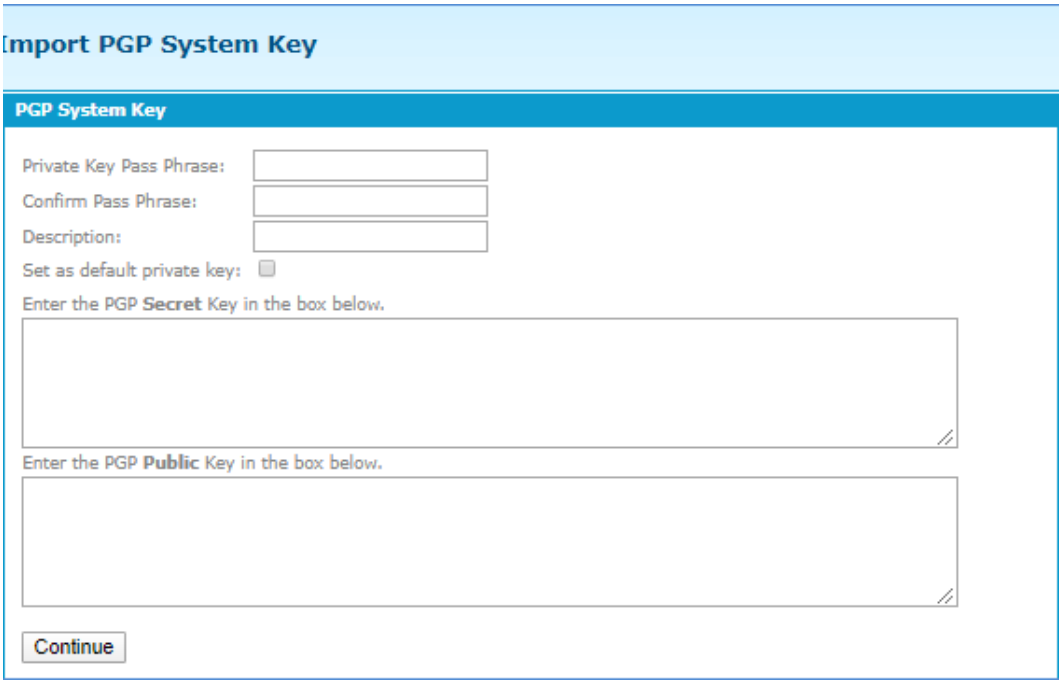
When the necessary fields are defined, you should click **Continue** to add the PGP system key to the MFT database.



Import PGP System Key

You can import PGP system keys through the Import PGP System Key page which can be accessed by clicking **Administration** > **PGP Keys** > **PGP System Keys** > **Import PGP Key**.

The following figure shows the Import PGP System Key page:

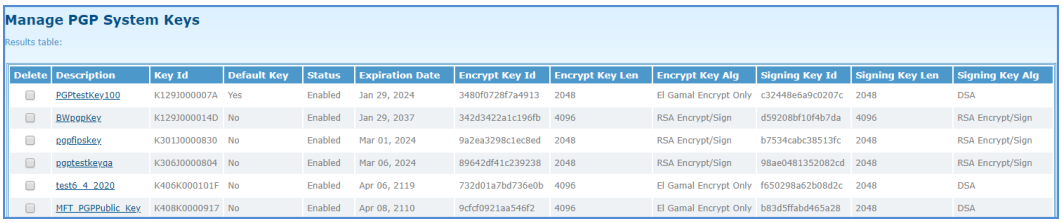


After defining the necessary parameters, click **Continue** to import the PGP system key to the TIBCO MFT Command Center database.

Manage PGP System Key

You can manage PGP system keys through the Manage PGP System Key page which can be accessed by clicking **Administration** > **PGP Keys** > **PGP System Keys** > **Manage PGP Key**.

The following figure shows the Manage PGP System Key page:



SAML

With the **Administration** > **SAML** option, you can import SAML identity provider metadata, configure SAML service provider metadata, and generate SAML service provider metadata.

Import SAML Identity Provider MetaData

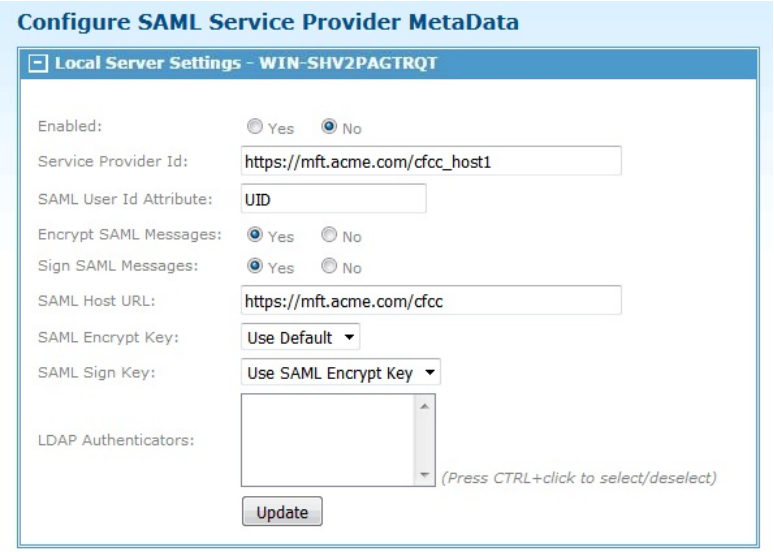
Click **Administration** > **SAML** > **Import SAML IDP MetaData** to import SAML identity provider metadata on the Import SAML Identity Provider Metadata page.

Copy and paste the SAML identity provider metadata into the **SAML Identity Provider MetaData** field, and then click **Import**. MFT will validate that the data is in a proper XML format and contains valid identity provider data.

There is a configurable box for TIBCO MFT Internet Server or TIBCO MFT Command Center that has been installed.

Configure SAML Service Provider MetaData

Click **Administration** > **SAML** > **Configure SAML SP MetaData** to configure SAML service provider metadata on the Configure SAML Service Provider MetaData page.



After entering the necessary information, click **Update** to update the database. For more information on how to configure SAML service provider metadata, see the online help page.

There is a configurable box for TIBCO MFT Internet Server or TIBCO MFT Command Center that has been installed.

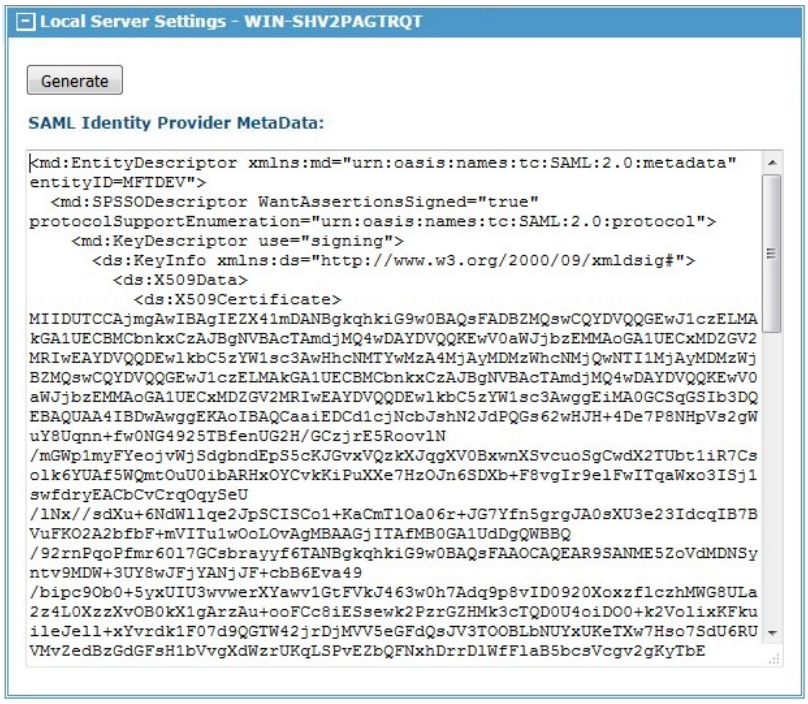
Generate SAML Service Provider MetaData

Click **Administration** > **SAML** > **Generate SAML SP MetaData** to generate SAML service provider metadata on the Generate SAML Service Provider MetaData page.

Click **Generate** to generate the service provider metadata. A text box that contains the service provider metadata is displayed.

There is a configurable box for TIBCO MFT Internet Server or TIBCO MFT Command Center that has been installed.

The following figure shows sample SAML service provider metadata:



Activity

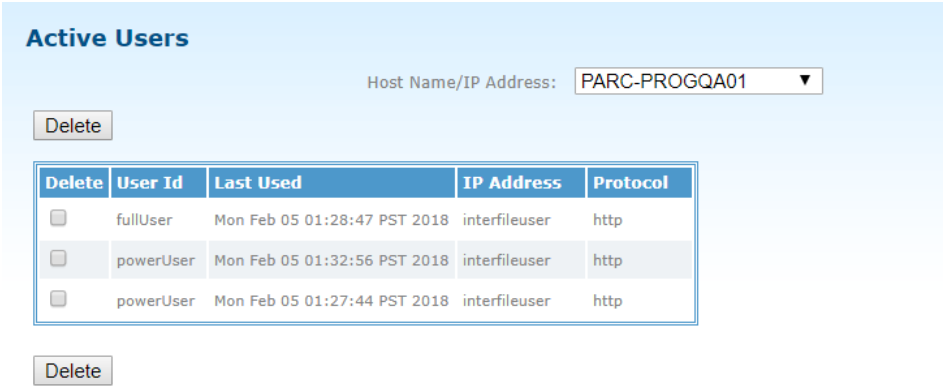
With the **Administration** > **Activity** option, you can view and manage the active sessions and checkpoints.

Active Users

Click **Administration** > **Activity** > **Active Users** to view and manage active sessions on the Active Users page.

Administrative users must have AdministratorRight or UpdateSessionRight to view the sessions.

This page displays all the active sessions in the system. The following figure shows the admin's session currently running.



To delete a user's session, select the check box next to the session that you want to delete and click **Delete**. Multiple sessions can be deleted at one time.

Internet Checkpoints

Click **Administration** > **Activity** > **Internet Checkpoints** to view and manage checkpoints on the Internet Checkpoints page.

This page displays all the checkpoints for all the transfers done using TIBCO MFT Internet Server. Users must have AdministratorRight to manage checkpoints.

This page contains a section, Selection Criteria, and a list of the first 100 checkpoints. If there are more than 100 checkpoints, click **List Next 100 >** to access the next 100 checkpoints. You can also click **Back** to see the previous Checkpoints.

A listing of particular checkpoints can be obtained by entering the search criteria for any combination of file ID, user ID, client file name, node name, server file name, transaction ID and proxy transaction ID. A percent sign (%) can be used as a wildcard character.

To delete a checkpoint, select the check box next to the checkpoint that you want to delete and click **Delete**. Multiple checkpoints can be deleted at one time.

Authenticators

With the **Administration** > **Authenticators** option, you can add and manage LDAP 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 Add Authenticator page and tested from the Manage Authenticators page. By default, the LDAP user's login ID, full name, email address (optional), and telephone number (optional) are pulled into the TIBCO MFT Internet Server database. In addition, to controlling user's details being pulled from the LDAP server, the administrator can optionally set up what TIBCO MFT Internet Server rights are assigned to those LDAP users.

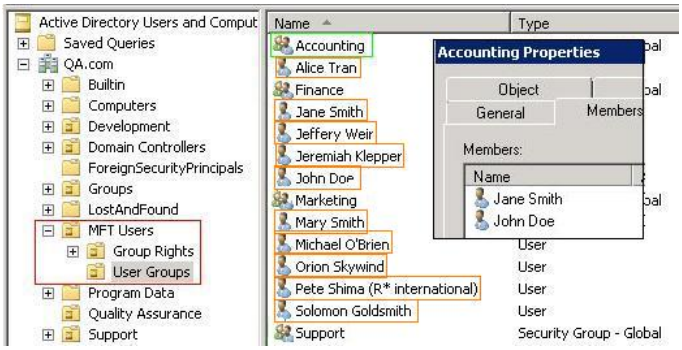
To add and manage LDAP authenticators, users must have TIBCO MFT Command Center AdministratorRight in the system.

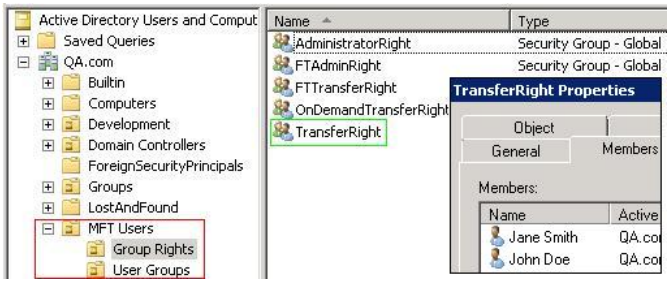
To allow TIBCO MFT Command Center to authenticate and synchronize with an LDAP server, you must have the following items on the LDAP server configured:

- You must know the host information, such as the IP and port of the LDAP servers that you will be authenticating to.
- You must know the Bind User DN and password.
- 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. The following figure is an example.
- You must know the User Base DN and Group Base DN where the sync group is located.

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

Example of the active directory setup:





Add Authenticator

Click **Administration** > **Authenticators** > **Add Authenticator** to add LDAP authenticators on the Add Authenticator page.

To synchronize the MFT database through LDAP, you must configure an LDAP authenticator. On the Add Authenticator page, you will see the Authenticator Properties section with the following subsections:

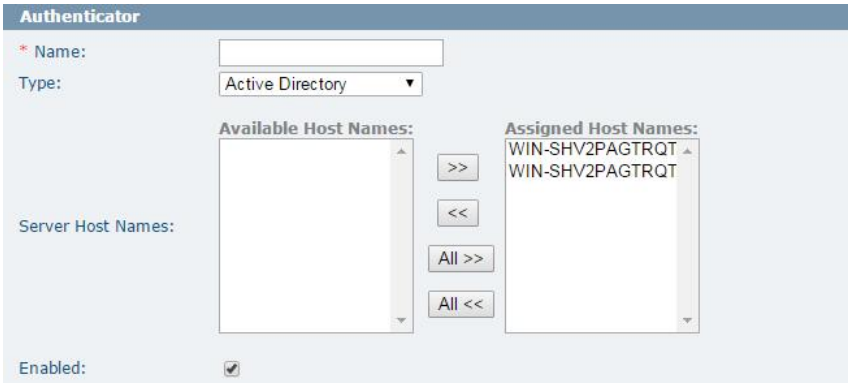
- Authenticator
- LDAP Connectivity
- LDAP Search
- LDAP Attributes
- Right Management

Authenticator

The **Server Host Names** area defines the servers that will use this authenticator. This area is split into two lists. The **Available Host Names** list displays the server host names that have not been assigned to an authenticator. The **Assigned Host Names** list displays the servers that have been assigned to an authenticator.

If there are no assigned host names, this authenticator will be used on all servers.

It is good practice 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 *authenticatorName-userID*. End users will not need this portion of the user ID to login to the system. For example, John Doe (jdoe) would login with jdoe and not AD162-jdoe.

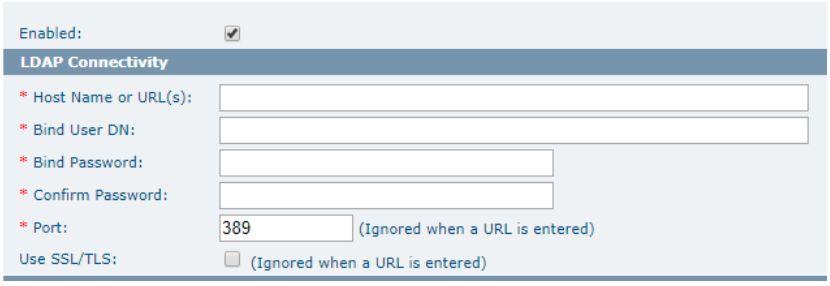


The following table lists the fields in the Authenticator section:

Field	Description
Name	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. For example, LDAPServer-john.doe.  This field cannot be specified 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.
Server Host Name	The hosts that will use this authenticator. If no specific host name is assigned, all the hosts will be set to use this authenticator.
Enabled	This parameter defines whether to enable this LDAP authenticator. If selecting this check box, 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 Update User page in TIBCO MFT Command Center or TIBCO MFT Internet Server.

LDAP Connectivity

This section defines the parameters are required to connect to the directory server and pull in the user and role information for synchronizing.



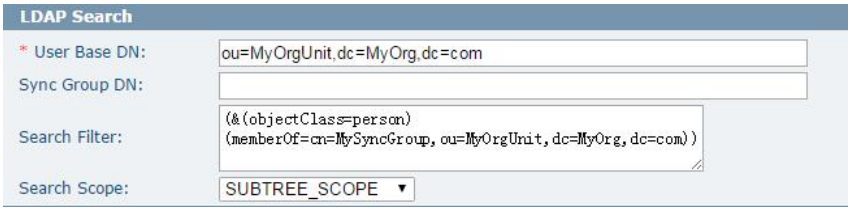
The following table lists the fields in the LDAP Connectivity section:

Field	Description
Host Name/IP Address/URL	Defines the host name or URL(s) of the LDAP Server. There are two ways to define this field: • Specify the Host Name or IP Address of the target LDAP Server. Define the LDAP Server IP Port in the Port field and use the "Use SSL/TLS" checkbox to define whether SSL/TLS will be used for connections to this LDAP Server. For example: your.ldap.server • Specify one or more LDAP URL(s). The LDAP URL must start with either "ldap://" or "ldaps://". You cannot mix "ldap" and "ldaps" in the same authenticator. Multiple LDAP URLs must be separated by a space. When you defined a URL, the "Port" and "Use SSL/TLS" parameters are ignored. For example: ldaps://your.ldap.server2:636 ldaps://your.ldap.server2:636
Bind User DN	The distinguished name required for authenticating to the LDAP Server.

Field	Description
Bind Password	The password associated with the defined Bind user.
Confirm Password	The 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	This parameter defines whether to enable using SSL. If the LDAP server you are connecting to is using SSL, you must enable this option. This parameter is ignored if a URL is specified in the Host Name or URL(s) field.

LDAP Search

The LDAP Search section defines the location of the sync group and the users which will be synced into the MFT database.



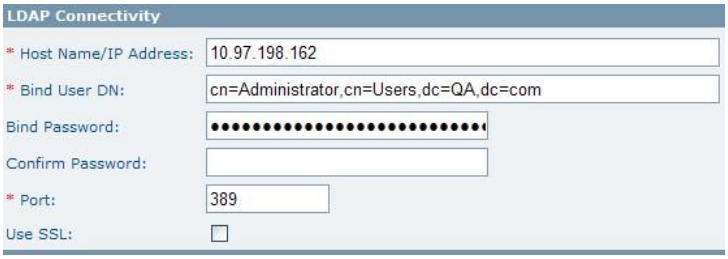
The following table lists the fields in the LDAP Search section:

Field	Description
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.

Field	Description
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.

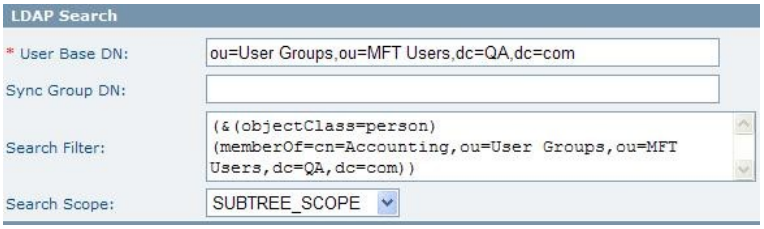
The following examples show different configurations that an administrator can set up to search for LDAP users:

Example 1: The following example will result in 10 Active Directory users being added to the MFT database:



Example 2: The following example will result in 2 Active Directory users being added to the MFT database:

Example 3: If you would prefer to use search filters we can accomplish the same results as in the above example using this setup:



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=*))
```

LDAP Attributes

This section defines the parameters that LDAP reads from the directory datastore server 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.

Right Management

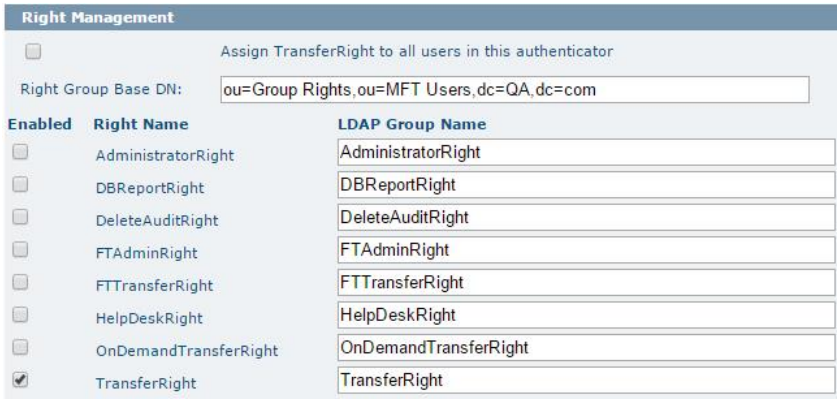
This section defines the rights you want to be managed using the LDAP server.

TIBCO MFT Command Center or TIBCO MFT Internet Server users can be assigned various rights which allow them different capabilities. The most popular of these rights is the Transfer right right; without this right assigned to a user, they cannot perform file transfers. After selecting the **Assign TransferRight to all users in this authenticator** check box, all users in this authenticator will be assigned with TransferRight when they are synced. When this check box is selected, you should not enable Right Synchronization for TransferRight. Some LDAP environments can want to control which users are assigned this right and other rights from the LDAP server. When the right is enabled for management through the LDAP server, it cannot be granted or un-granted from TIBCO MFT Command Center or TIBCO MFT Internet Server. A group with the name which is specified in the **LDAP Group Name** field must exist on the directory server and the users granted this right must be members of the group.

The following table lists the fields in the Right Management section:

Field	Description
Right Group Base DN	The location in the directory tree of the OU which contains the MFT rights.
Enable	This parameter defines whether to enable the right 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 in the LDAP server that will be associated with the right in MFT. This name 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.

The following example will result in 2 Active Directory users being added to the MFT database:



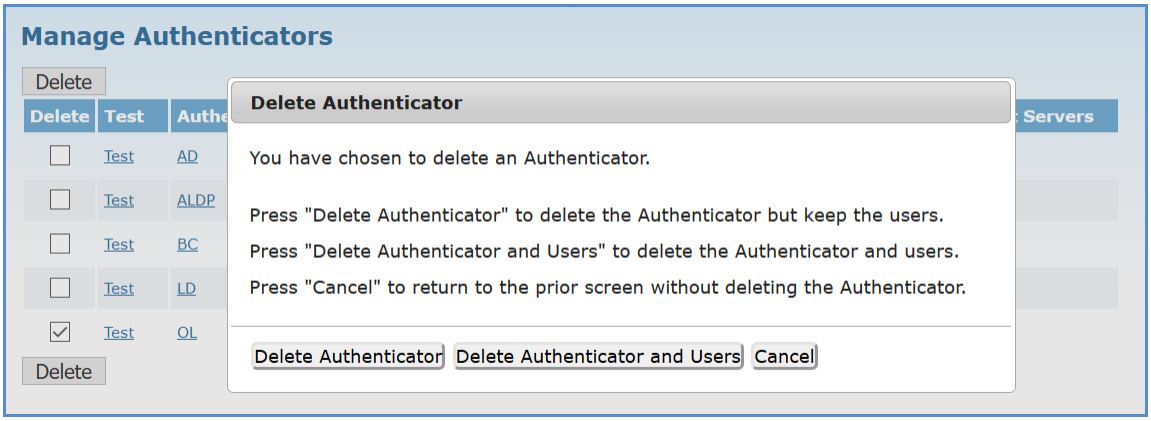
Manage Authenticators

Click **Administration** > **Authenticators** > **Manage Authenticators** to manage LDAP authenticators on the Manage Authenticators page.

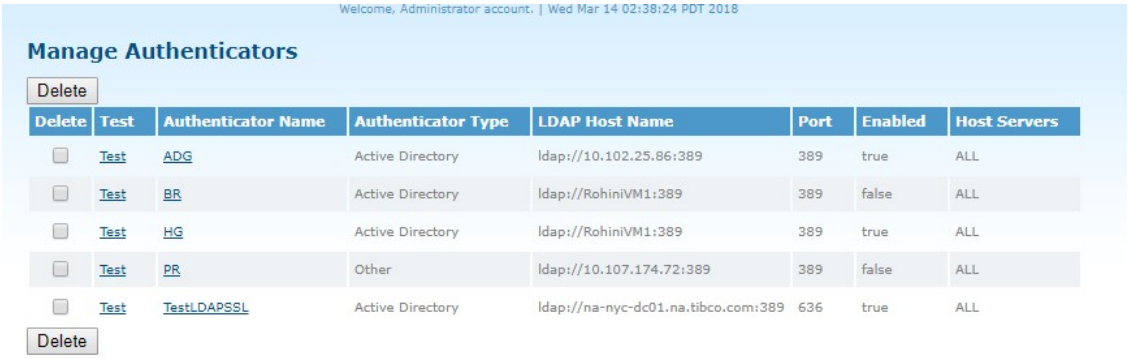
On the Manage Authenticators page, you can update, delete, or test authenticators.

To update an authenticator, click the authenticator name link to open the Update Authenticator page. When the changes are made, click Update to save the changes.

To delete an authenticator, click the authenticator name link that you want to delete and the Delete Authenticator page is displayed. You are prompted to define whether the authenticator should be deleted or the authenticator and all authenticator users should be deleted.



To test an authenticator, click **Test** next to the authenticator name that you want to test the connection for.



Click **Test** to verify connection settings and returned results with TIBCO MFT Internet Server. The following shows 2 users will be synchronized with the MFT database along with the TransferRight assignment:

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 MFT administrator to assign rights to the users through the TIBCO MFT Internet Server Administrator web pages.

LDAP Sync

To populate the MFT database with LDAP users, you should sync TIBCO MFT Internet Server with an LDAP server. To bind to the LDAP server, you should set up an authenticator through the **Administration** > **Authenticators** > **Add Authenticator** option.

See Add Authenticator for more information. When the authenticator is configured and tested, you can run an LDAP sync.

By default, synchronization to the TIBCO 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 the right management is enabled on the authenticator.

To synchronize LDAP authenticators, a user must have TIBCO MFT Command Center AdministratorRight assigned to them in the system.

Synchronization is performed three different ways:

- Manual Sync

  A manual sync can be done by the administrator by going to the LDAP Sync page to sync a single user or all LDAP users.

- Scheduled Sync

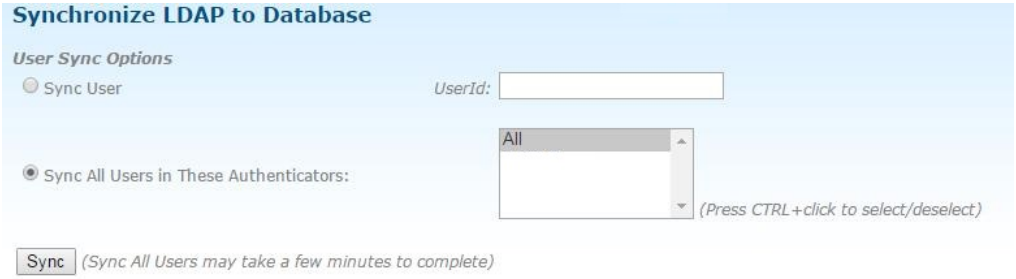
  A scheduled sync can be done once a day by setting up the options found in the LDAP Settings section of the Administration > System Configuration page. By default, this is disabled. If you have TIBCO MFT Command Center and TIBCO MFT Internet Server sharing the same database the sync can be configured to be performed by either server.

- Automatic Sync

  This synchronization occurs when an LDAP user logs into the TIBCO MFT Command Center system and authenticates against the LDAP server.

Manual Sync

In this case, synchronization is manually executed by Super Administrator. To synchronize, log into TIBCO MFT Command Center or TIBCO MFT Internet Server Administratior web page and go to the Administration > LDAP Sync page. This form gives two options for synchronizing. The administrator can sync a single user or all users across all active authenticators or a selected group of authenticators.



To synchronize a particular user, Click **Sync User**, enter the user ID of the user that you want to sync and then click **Sync**.

Sync All Users in These Autheticators

To synchronize all users and all roles for the defined authenticators, click **Sync All Users in These Authenticators**. By selecting **All**, all users in all authenticators will be synced. Alternatively, you can select a single authenticator by clicking that authenticator. You can also select multiple authenticators. Any users defined to LDAP but not to Internet Server will be added to Internet Server. Any user defined to Internet Server but not to LDAP will be disabled. Any user whose LDAP attributes are different than the database attributes, will be synchronized. Additionally, Internet Server will check all Internet Server roles defined to LDAP to ensure that they are synchronized with the Internet Server rights.

This option can take a few minutes to complete when a large number of users are defined by the LDAP authenticators.

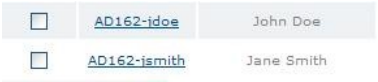
When you have selected the action that you want to perform, click **Sync** to start the synchronization process.

The synchronization options can take a few minutes to complete. Do not click **Sync** until the previous sync has completed.

The total amount of LDAP users and rights (if enabled) synchronized will be displayed at the top of the page.

If an error occurs for one user, the sync will continue on to the next user.

When you have synchronized the LDAP users, the administrator can go to the Manage Users page where they will see the new LDAP users added to the system. The following figure shows two LDAP users added to the system:



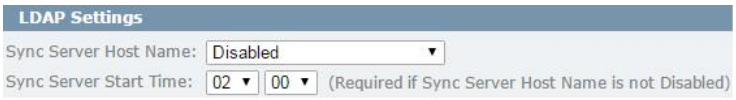
When LDAP user IDs are synchronized,, they will be represented in the MFT database in the format of *AuthenticatorName*-userid. End users will not need the authenticator name to login to the system. For example, John Doe (jdoe) would login with jdoe and not AD162-jdoe.

The new users synchronized can now login to MFT using several different user Id options. For example, jdoe and QA\jdoe, which is using the LDAP domain.

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\user ID that they want to connect with.

Scheduled Sync

To set up LDAP synchronization to be done daily, go to the System Configuration page.



In the LDAP Settings section, first select the server that you want to perform the synchronization from the **Sync Server Host Name** list. By default this is set to `Disabled`. If you do not have multiple TIBCO MFT Internet Server servers sharing the database, you only see one server in the list.

Then, set the sync server start time.

Finally, click **Update** when you are done to save you configurations.

Automatic Sync

An automatic sync occurs every time an LDAP user logs in to the TIBCO 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.

Lockout

With the **Administration** > **Lockout** option, you can release the locks that has been placed on users, IP addresses, or the system.

Users must have AdministratorRight to release locks for users, IP addresses and the system. When a lockout will occur is configured in the Global Lockout Rules section on the System Configuration page.

Lockout Management

Click **Lockout** > **Lockout Management** to release the locks that has been placed on users, IP addresses, or the system on the Lockout Management page.

To release the lock on a single IP address, the operation is the same as a single user account.

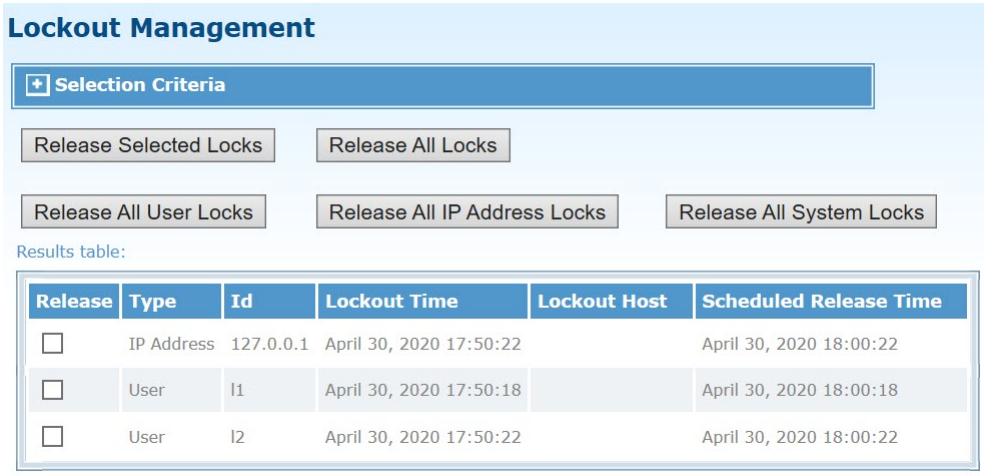
You can release more than one user account or IP address by typing them in separated by a semi colon (;) as shown in the following example:

```
10.97.196.26;10.97.196.101
```

The user IDs or IP addresses entered are not validated.

To release locks for users, IP addresses, and the system, you must have AdministratorRight.

The following figure shows the Lockout Management page:

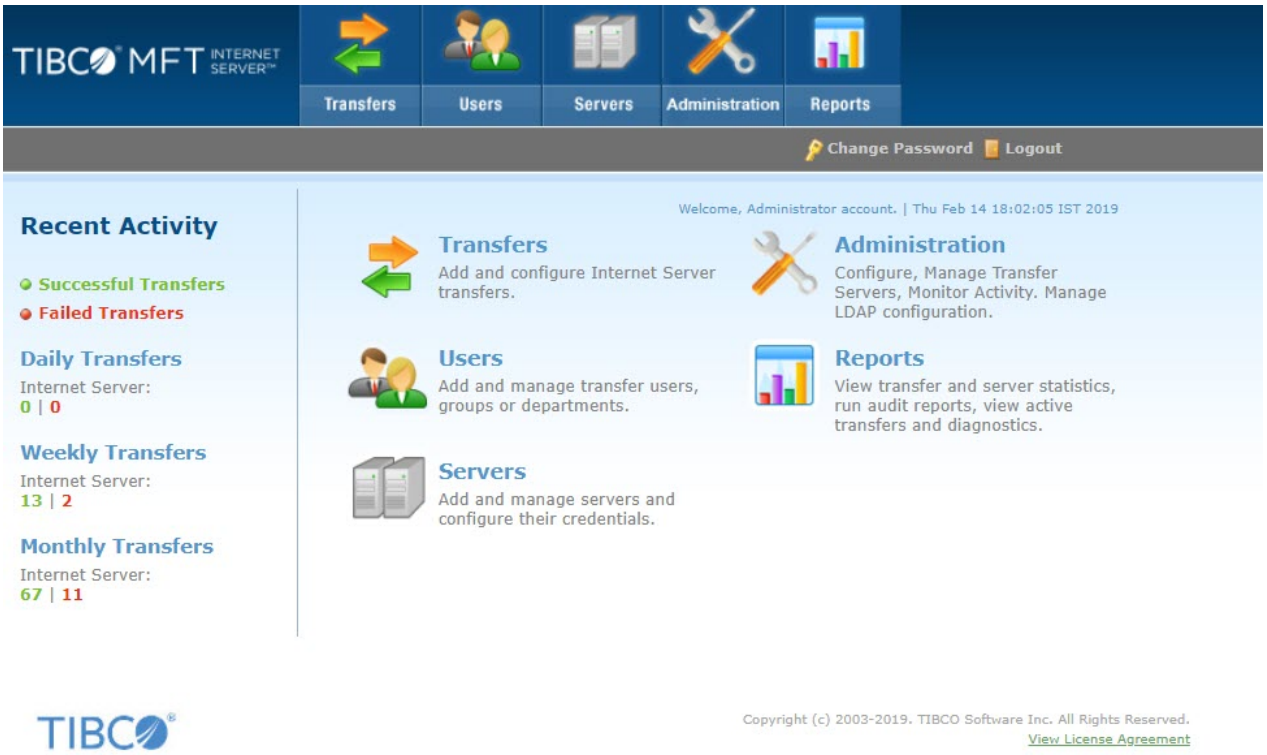


By default, the Lockout Management page displays all current lockout users, IP addresses, and systems records in a table list. This page displays up to 500 locks at a time. If more than 500 resources are locked, use the **Selection Criteria** field to filter the locks you want to display. **Selection Criteria** allows you to search for locks based on lock type or lockout ID name.

Locks are only accumulated when the systems configuration **`Maximum Number of Failed Logon Attempts`** parameters are set to a non-zero value for the system, IP address, and the user. Restarting the web server clears all locks.

Reports

With **Reports** option, you can view transfer and server statistics, run audit reports, view active transfers ans diagnostics.



Audits

With the **Reports** > **Audits** option, an administrator can search, delete, and save specific search criteria in a filter for audit records generated by TIBCO MFT Internet Server audit logs.

Search Audits

Click **Reports** > **Audits** > **Search Audits** to search for completed TIBCO MFT Internet Server transfers on the Search Audits page.

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 **List Next 100 >** to access the next 100 audit records.

If you want to conduct a more detailed search through the audit records, use the Selection Criteria section 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 (%) can be used as a wildcard character in all the fields.

To view all the details of an audit record click 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 TIBCO MFT Internet Server transfers are conducted.

Platform Server Manual Poll (Command Center Only):

To run a Platform Server Manual Poll on remote Platform Server, it must have a server definition in TIBCO MFT Command Center with a server type of Platform Server. This server definition must have the **Manage Platform Server** check box selected under the **Management** option (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 Platform Server in real time and bring it forward for you to view now.

Delete Audits

Click **Reports** > **Audits** > **Delete Audits** to delete audit records on the Delete Audits page.

Audit records contained in the database can be deleted. To delete audit records, an TIBCO MFT Internet Server user need either AdministratorRight or DeleteAuditRight to delete audit records.

To delete audit records, select a date or number of days as well as the audit type, and then click **Delete**.

Audit Search Filters

With the **Reports** > **Audits** > **Audit Search Filters** option, you can add and manage audit search filters.

An administrator can configuration the Selection Criteria section on Search Audits page to define exactly what audits he wants to view but this search criteria cannot be saved. The audit search filters allows an administrator to define a search criteria, and then save it to be used over and over again.

Users must have either AdministratorRight or FTAdminRight to add or manage audit search filters. See the online help page for detailed information on each field available to be configured on the Add Audit Search Filter and Manage Audit Search Filters pages

Add Audit Search Filter

Click **Reports** > **Audits** > **Audit Search Filters** > **Add Audit Search Filter** to pre-define the selection criteria used to display TIBCO MFT Internet Server and Platform Server audit records on the Add Audit Search Filter page.

In the Audit Search Filter Selection Criteria section, you can define filters to limit the number of audit records that will be displayed. When the selection criteria is completed, click **Add** to add the entry to the audit search filter.

To execute an audit search filter, click **Reports** > **Audits** > **Search Audits** and select the filter from the **Retrieve pre-selected filter** list in the Selection Criteria section.

Manage Audit Search Filter

Click **Reports** > **Audits** > **Audit Search Filters** > **Manage Audit Search Filter** to update a audit search filter you have saved in the system on the Manage Audit Search Filter 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 **List Next 100 >** to access the next 100 audit filter definitions.

To update an audit search filter definition, click the search audit ID of the definition that you want to change. Make the changes, and then click **Update**.

To delete an audit search filter definition, select the check box next to the search audit ID that you want to delete, and then, click **Delete**. Multiple audit search filters can be deleted at one time.

Diagnostics

Click **Reports** > **Diagnostics** to view the information that assists TIBCO Support in solving issues with TIBCO MFT Internet Server on the Diagnostics page.

If you want to save the diagnostics, click **Save Server Diagnostics to File** to save it to the local disk. The exact page format and the location of the file are dependent on the web browser that you are using.

The Diagnostics page contains the following information:

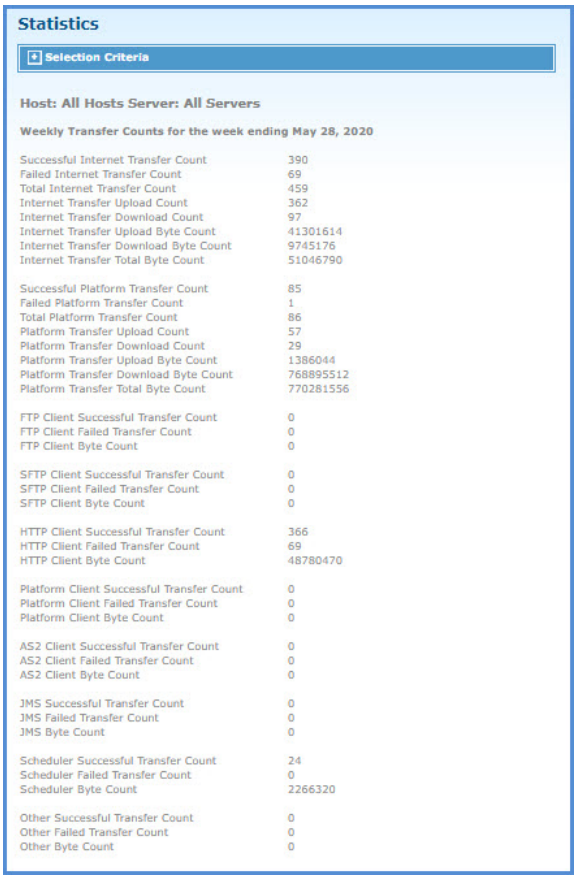
section	Description
Version Information	Displays the information about the version and build, as well as the J2EE server type and version.
Install Paths	Displays the path where Internet Server was installed.
Database Info	Displays the number of active database connections.
JVM Settings	Displays JAVA Virtual Machine memory usage and FIPS settings.
Active Transfers	Displays information about currently active transfers.
Server Time Settings	Displays the current time on the remote server and on the local server.
Active Trace Object Count	Displays information about trace object count.
JVM System Properties	Displays information about the Java virtual machine (JVM).
Environment Variables	Displays the system defined properties that are used with Tomcat and are found in the JAVA_OPTS environment variable.

section	Description
SSL Ciphers Suites	Displays SSL/TLS ciphers supported by the JVM.
Web.xml Context Parameters	Displays information located in the Web.xml file.
Trace Setting	Displays the internal tracing information for transfer definition IDs, users, or servers.
File Information	Displays the path and date/time of files located in the application context as well as important Java files.
Trace Info	Displays information about internal tracing.
Session Info	Displays information about the current number of sessions.

Statistics

Click **Reports** > **Statistics** to view daily, weekly and monthly transfer byte counts and more on the Statistics page. You can search and get information with regard to the activity on the Command Center and the Internet Server systems through this page.

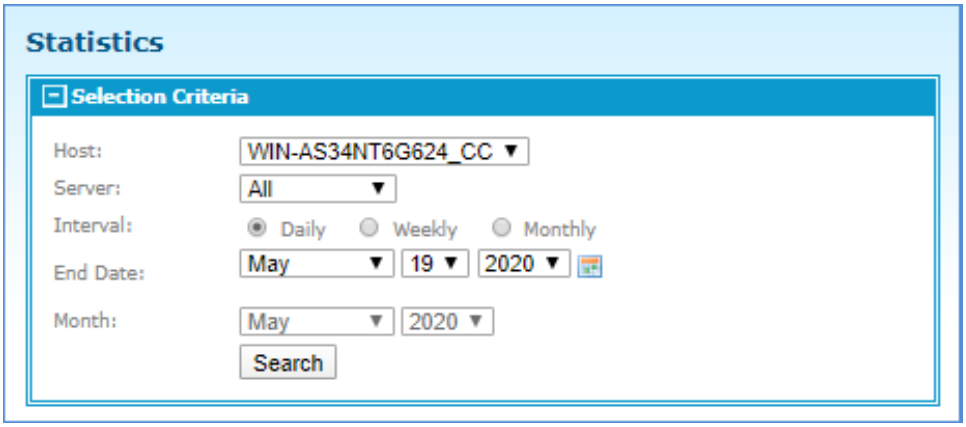
The following figure shows a list of the various details on the Statistics page:



The Selection Criteria allows you to display transfer statistics by a variety of criteria, such as the host where the transfer executed (for Platform Servers, this is the Command Center where the audit records were collected) or the server where the transfer executed. (For Internet Server, this is the target **Server Name**

defined in the transfer definition. For Platform Server, this is the **Server Name** associated with the Platform Server collection.)

The following figure shows the Selection Criteria section:



Error Events

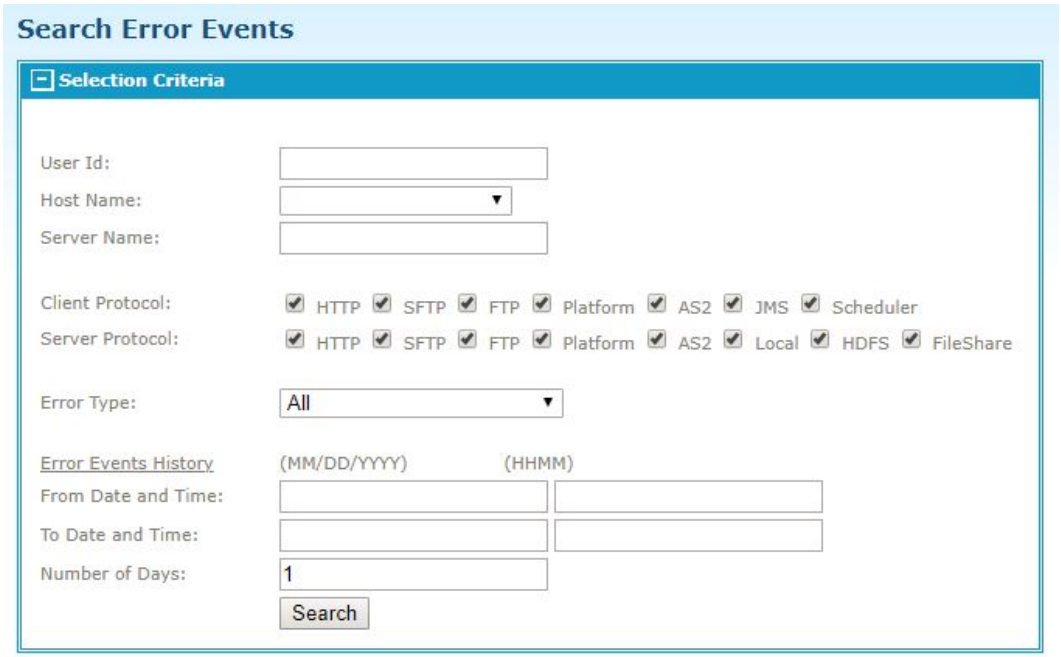
Error events are written when errors are detected in normal processing, but audit records might not be written. Error events can help you perform problem determination without taking traces. You can search for error event detected through the **Reports** > **Error Events** option.

Search Error Events

You can search for error events detected through the Search Error Events page which can be accessed by clicking **Reports** > **Error Events** > **Search Error Events**.

By default, up to 500 error event records can be displayed in the Results table on the Search Error Events page.

You can define selection criteria in the Selection Criteria section to limit the number of events that are displayed in the Results table. The following figure shows the Selection Criteria section:



You can use a single field or a combination of fields to define the selection criteria. The percent sign (%) can be used as a wildcard character in all the fields. The information entered in the Selection Criteria section is

matched against the records in the TIBCO MFT Internet Server database. Only error event records that match all the parameters defined in the selection criteria will be displayed.

Admin Changes

You can search for admin changes generated through the **Reports** > **Admin Changes** option.

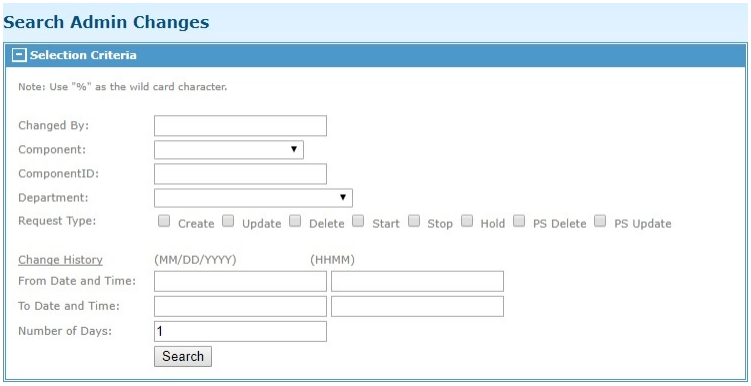
All admin changes are logged. If there are admin changes that you do not want logged, you can configure it through a file in the WEB-INF folder called: `PCISkip.xml`. This file allows you to enter components and field names where changes can be ignored. You can turn on this checking by updating the web.xml property: **`PCISkipFileName`**. This parameter points to the `PCI Skip` file; the default file name is `PCISkip.xml`. You must edit this file and add components and field names. If the only admin changes are fields defined in this file, then the change will not be logged. The reason is that some users may not want to log all changes. If there is a batch process where, for example, the User Disabled flag is frequently turned off and on, you may not want to write an Admin Change record each time this field is updated. If you add this to the PCISkip.xml file, User updates where the Disabled flag is the only field changed will not be logged.

If you update the PCISkip.xml file, you must restart the MFT Server.

Search Admin Changes

You can search for admin changes through the Search Admin Changes page which can be accessed by clicking **Reports** > **Admin Changes** > **Search Admin Changes**.

By default, the Search Admin Changes page up to 500 Admin change records are displayed within the Results Table. The Selection Criteria box allows you to filter the admin changes to limit the number of admin changes that are displayed in the Results Table. The following figure shows the Search Admin Changes page:



You can use a single field or a combination of fields to define the selection criteria. The percent sign (%) can be used as a wildcard character in all the fields. The information entered in the Selection Criteria section is matched against the records in the TIBCO MFT Internet Server database. Only admin change records that match all the parameters defined in the selection criteria are displayed.

Help

Each web page contains a **Help** link. You can click it to obtain more information about the web page and field configuration.

Miscellaneous Parameters

Miscellaneous parameters refer to parameters that do not fit into the other categories.

The following table lists the miscellaneous parameters:

Parameter	Default	Description
AlertCheckInterval	60	Defines the interval in seconds between checks to see if the Alert Cache needs to be updated. Valid values are from 1 to 60 seconds, and the default value is 60 seconds. You should change this parameter only if you need to lower the elapsed time between when an alert is added, deleted or updated, and when the alert cache is updated.
AssignViewEmailContentsRight	admin	This parameter is not used.
AuditDir	The directory defined during installation	Defines the directory where MFT audit files are located.
CacheTimeStampInitYieldSec	120 seconds plus a random number between 1 - 60 seconds	Defines the amount of time that Internet Server and Command Center waits at startup time before monitoring for cache updates and inactive hosts.
CacheTimeStampIntervalSec	30 seconds	Defines how frequently Internet Server and Command Center check for cache updates. It also defines how frequently Internet Server and Command Center check for inactive hosts. For more information on deleting inactive servers, see the **CacheTimeStampRemoveHostThreshold**.

Parameter	Default	Description
CacheTimeStampRemoveHostThreshold	20 intervals	Defines how many times an Internet Server or Command Center allows a server to be inactive before removing the host from the database. MFT checks if a server is active based on the **CacheTimeStampIntervalSec** parameter. If a server is inactive for the number of times defined by this parameter, the host is removed from the database. This parameter is used only when the Internet Server or Command Instance is a dynamic Cloud instance started with the COM_TIBCO_MFT_CE_TEMPLATE NAME environment variable.  Only Command Centers or Internet Servers with the administrator service installed check for inactive servers.
DefaultTransferClient	browser	Defines the default transfer client. The value of `browser` indicate the default transfer client is the browser client. It is good practice to use the browser client by default. The value of `java` indicate the default transfer client is the Java client.
EmbeddedServer	`true`	This parameter should always be set to `true`.
ExpiredFilesLog	`./ExpiredFilesLog.txt`	This parameter is not used.
HTTPOnlyCookies	`True`	If set to true, all cookies created by MFT will have the HTTPOnly attribute set. By default, httponly is set for MFT generated cookies. There are a few cookies that do NOT have httponly set, because the JavaScript requires these cookies. The cookies that do NOT have httponly set do not contain any privileged or sensitive information.

Parameter	Default	Description
HostName	The host name defined during installation	Defines the host name that was set during the configuration process. This parameter is used to identify the MFT server in the database tables. This should not be changed without guidance from Technical Support.
HttpSSOCustomizationConfigFile	No default	Defines the HTTP SSO customization file. This should only be used when the server is configured to support SSO. Generally, this parameter is set to the SSO configuration file, `httpssocustomization.xml`.
ISCCFlag	None	Set at installation time and notifies the MFT Cloud Servlet whether this installation is for Internet Server or Command Center. The value of this parameter should not be changed
MaximumFileNumber	`10000`	Defines the maximum number of files to be returned to the browser or Java client for a single directory scan.
MessageDir	The directory defined during installation	Defines the directory where MFT message files are located.
MinimumJREVersion	`1.7.0+`	Defines the minimum JRE version for the Java file transfer applet. If the version is less than this value, the user is prompted to upgrade the Java version.
PCISkipFileName	No default	Defines the name of the PCI file that can be used of if you want to skip "Admin Change" logging for a particular field in an object. Refer to file "PCISkip.xml" for details on how to configure this file.
S3ClientConfigFile	No default	Defines the S3 config file name.  Do not change this parameter unless instructed to do so by MFT Technical Support.

Parameter	Default	Description
SAMLAuthenClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:Password	Allows users to update the **SAMLAuthenClassRef** used in the SAML negotiation.  Only do this if you are using a non-standard SAML Authentication Class Ref and are instructed by MFT Support to change this field.
SAMLComparison	MINIMUM	Allows users to update the SAML Comparison method. The default value of MINIMUM is suggested. Other supported values are: EXACT, MAXIMUM, or BETTER.  Only change this field if you are instructed to do so by MFT Support.
SAMLNameIDType	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	Allows users to update the **SAMLNameIDType** used in the SAML negotiation.  Only do this, if you are using a non-standard SAML name ID type and are instructed by MFT Support to change this field.
SearchAuditAtPageEntry	true	Defines whether MFT performs an audit search when the Search Audits page is first configured. The value of true indicates that MFT performs an audit search when the Search Audits page is first configured. The value of false indicates that MFT does not perform an audit search when the Search Audits page is first configured. Searches will be on demand when the user defines the selection criteria and click **Search**.
SendGlobalEmail	true	This parameter is not used.

Parameter	Default	Description
SendMFTTrustedCerts	false	True: When an FTPS client connects to the MFT FTPS Server, MFT returns a list of certificates that are defined to MFT as "Trusted Certificates". False: MFT does not send any trusted certificates to the FTPS Client.
SoapSkipFieldsConfigFileName	No default	When a customer uses SOAP calls and wants to upgrade MFT to a different version, setting this parameter will tell the SOAP calls to be compatible with older versions of MFT. Any RETRIEVE or GET call returns data in the format defined by MFT 7.2.4.
StatisticsUpdateInterval	10	MFT asynchronously updates the DB MFTStatistics table to improve performance. This parameter defines the frequency of statistics updates.
SyncLdapAtLogon	true	Defines whether an LDAP user will be synced with the LDAP authenticator when HTTP users log on. The value of True indicates that LDAP users are synced when the user logs on. The value of False indicates that LDAP users are not synced with the LDAP authenticator when the user logs on. The sync is performed when the On Demand or scheduled sync occurs.
TraceDir	The directory defined during installation	Defines the directory where MFT trace files are located.
TransferJMSThreadPoolSize	100	Defines the number of threads that is used to execute JMS Internet Server or Platform Server transfer requests. This parameter limits the number of concurrent JMS initiated transfers to the defined value.

Parameter	Default	Description
ValidationQueryTimeout	1	Defines the number of seconds that MFT waits for a DB Pooling validation query. If the query does not return in the defined number of seconds, the connection is closed and a new connection is created.
WebAdminLogFile	The directory defined during installation	Defines the directory where MFT WebAdmin files are located.
crystal_image_uri	/cfcc/control?view=view/cfcc/crystalreportviewers11	Defines the URL for the MFT reporting application.
net.sf.jasperreports.web.file.repository.root	No default	Defines the JasperSoft report root.  Do not change this parameter unless instructed to do so by MFT Technical Support.
reuseJMSConnection	false	True: Reuses JMS connections. False: Creates a new JMS connection for each request.  This parameter should be used for EMS only.
tilesDefinitions	/WEB-INF/tiles.xml	This parameter should not be changed.

Delegated Administration

Delegated administration offers an TIBCO MFT Internet Server administrator the ability to divide the system into smaller units that 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 administrator's department and the departments that this administrator can manage. They cannot administer anything else in the system. The existing system rights, such as UpdateTransferDefinitionRight, can also be applied to department administrators thus offering a finer granularity of administrative control.

Administrators who are not assigned to a department are considered as super administrators who can manage the entire system. While department administrators can only access their own departments and the departments they can manage, super administrators have access to all departments in the system. They are the only ones who can administer 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 server is assigned.

An administrator can further limit the access to his users, groups and servers through the use of visibility. The 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.

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.

Active Users

The following table lists the tasks that users can perform on active users.

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

User	Task
Department Administrator	A department administrator with ViewSessionRight can only view active users in his own department and the departments that the administrator can manage. A department administrator with UpdateSessionRight can delete and view active users in his own department and the departments that he can manage.
Super Administrator	views or deletes active users.

Audits

The following tables list the tasks that users can perform on audits records.

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 in his own department and the departments that he can manage. The exception to this rule occurs when a department administrator does searches on audit records. A user with ViewAuditRight can perform audit searches.

Search Audits

User	Task
Department Administrator	Searches for and displays audit records that have been in this administrator's department and the departments that the administrator can manage. When performing a search based on user ID, group ID or server name, only those that have been in this administrator's department and the departments that the administrator can manage can be used as the search criteria. A department administrator will only be able to view the audit records of file transfers in his own department and the departments that he can manage, 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. This extended search capability is provided as a convenience for department administrators.
Super Administrator	Searches for and displays all audit records in the system.

Delete Audits

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

Departments

The following tables list the tasks that users can perform on departments.

The department administrative tasks can only be performed by super administrators. A department administrator can only manage the users in his own department and the departments that he can manage.

Add Department

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

Manage Department

User	Task
Department Administrator	Cannot perform this task.
Super Administrator	Lists, updates and deletes all departments in the system.

Diagnostics

Only super administrators can view the diagnostics.

FTP Server Configuration

Only super administrators can perform FTP server configuration.

Groups

The following tables list the tasks that users can perform on 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 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 droup ID in a file transfer definition that is assigned to other departments. The group can be used as the group ID 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 super administrator updates a group originally created by department administrators, then only the information that department administrators have 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.

Add Group

User	Task
Department Administrator	Creates a group, which is assigned to this administrator's department or the department that the administrator can manage. 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.

Manage Groups

User	Task
Department Administrator	Updates and deletes any groups that have been in the administrator's department and the departments that the administrator can manage. Department administrators can see and change the **Department** parameter of a group definition assigned to their departments and the **Department** parameter of a group definition assigned to any departments that they can manage. The visibility of the group can be changed to public or private by department administrators.
Super Administrator	Lists, updates and deletes 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.

Internet Checkpoints

Only super administrators can perform this task.

Transfers

The following tables list the tasks that users can perform on transfers.

Transfers can be assigned to departments. A transfer can be assigned to only one department in the system. The super 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 super administrators. Transfers do not have a visibility associated with them. A department administrator can access or view transfers in his own department and the departments that he can manage. 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 in his own department and the departments that he can manage as well as users, groups and servers from other departments that have a visibility of public. If super administrators updates a transfer definition originally created by department administrators, then only the information that department administrators have access to can be used. Otherwise, an error will occur. Care should be taken when changing the department on a transfer definition. The user, group and server visibility need to be considered.

UpdateTransferDefinitionRight enables a user to add, update, delete and view transfers.
ViewTransferDefinitionRight enables a user to view an internet transfer definition.

Add Transfer

User	Task
Department Administrator	Creates a transfer that is assigned to the administrator's department and the departments that the administrator can manage. When selecting the authorized user ID, group ID, or server, only users in the same department and the departments that the administrator can manage, as well as groups, or servers from other departments with public visibility can be used.
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.

Add From Existing Transfer

User	Task
Department Administrator	Creates a new transfer that is assigned to the administrator's department and the departments that the administrator can manage. The new transfer can only be created from a pre-existing transfer from the same department and the departments that the administrator can manage. When selecting the authorized user ID, authorized group ID, or server, only users, groups, or servers which are in the same department and the departments that the administrator can manage, and 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 servers, it can be any user, group, or server assigned to the chosen department or any public user, group, or server from another department.

Manage Transfers

User	Task
Department Administrator	Lists, updates and deletes transfers that are in the administrator's department and the departments that the administrator can manage. When selecting the authorized user ID, authorized group ID, or server, only the users, group, or servers in the same department and the departments that the administrator can manage can be used, and 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 Super administrators can change the department a transfer has been assigned to.
Super Administrator	Lists, updates and deletes any internet transfer definition in the system. When updating the authorized user ID, group ID, or server, only user IDs, 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. Super Administrator will see all information in the pull-down menus, but he must comply with the rules stated above for Department Administrator or an error will occur. Only super administratora 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.

Server

The following tables list the tasks that users can perform on servers.

Servers can be assigned to departments and they can have a public or private visibility. Super administrators will be the only one who can perform the tasks of creating and configuring servers and assigning them to the particular department.

Department administrators cannot add servers. Department administrators can list all servers defined to their departments and all servers assigned to the departments they can manage. Department administrators can update servers assigned to their departments or the departments they can manage.

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 his own department and the departments that his department administrator can manage. 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 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 update and view servers. ViewServerRight enables a user to view a server.

Add Server

Administrator	Task
Department Administrator	Cannot perform this task.

Administrator	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.

Update Server

Administrator	Task
Department Administrator	Department administrators can update servers assigned to their departments and servers assigned to the departments that they can manage. The department to which the server is assigned can be changed to the department administrators' departments or any departments that the department administrators can manage.
Super Administrator	Updates and deletes 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.

Server Credentials

The following tables list the tasks that users can perform on server credentials.

Administrative tasks associated with severs credentials can be limited by the rights that are assigned (or not assigned) to a user. Department administrators cannot administer server credentials unless they are given UpdateServerCredentialRight. Otherwise, super administrators will be the only one who can perform these tasks. Public users and groups associated with server credentials can only be mapped to servers that are in their departments and the departments that their department administrators can manage, 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.

Add Server Credentials

Administrator	Task
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.

Manage Server Credentials

Administrator	Task
Department Administrator	Lists, updates and deletes server credentials if they are given the proper rights. In addition to AdministratorRight, administrative users must also be given UpdateServerCredentialRight to perform this function.
Super Administrator	Lists, updates and deletes any server credential definition in the system.

Statistics

Only super administrators can perform this task.

System Configuration

Only super administrators can perform these tasks.

Users

The following tables list the tasks that users can perform on 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 in his own department and the departments that his department administrator can manage, he can be set as the authorized user of transfer definitions that have been in his own department and the departments that his department administrator can manage, and he can have a server credential created for public and private servers in his own department and the departments that his department administrator can manage. 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.

Add User

Administrator	Task
Department Administrator	Creates users with TransferRight (default) who are automatically assigned to the administrator's department. Department Administrator can also create users who are assigned to the administrator's department or the department that he can manage, and who can have any one of the system administrative rights within the department. This means department administrators cannot create super administrators, 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 other department administrators in the system.
Super Administrator	Same as department administrators but the user can be assigned to any department in the system or to none at all. Super administrators 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 super administrators.

Add From Existing User

Administrator	Task
Department Administrator	Using this feature, a 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 or the department that he can manage. The new user will automatically be given rights depending on the user that is being used as a template. However, Department administrators 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, super administrators 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.

Manage User

Administrator	Task
Department Administrator	Updates users who have been in the administrator's department and the departments that the administrator can manage. Department administrators can change the department to which that the user is assigned to their own departments or to any departments that they can manage. Visibility of the user can be changed to public or private by the department administrator.
Super Administrator	Lists, updates and deletes 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.

Extended Features

TIBCO 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 Command Line Client Utility (as known as Admin Client Utility) and Internet Server Command Line Client Utility (also known as Internet Transfer Client Utility).

TIBCO MFT Internet Server Utilities

TIBCO MFT Internet Server provides the Administrator Command Line Client Utility and Internet Server Command Line Client Utility. The two command-line utilities can be invoked from a batch file, a UNIX script, as well as executed in unattended mode by a job scheduler for ease of use. TIBCO MFT Internet Server also provides a Promotion Utility that can be invoked from the command line and the GUI using a batch file or a UNIX script.

See *TIBCO Managed File Transfer Internet Server Utilities Guide* for more information about installing and configuring TIBCO MFT Internet Server utilities.

Executing TIBCO MFT Internet Server File Transfer as a Post Processing Action

Post processing actions allow you to perform up to four actions to be completed by the responding server when a file transfer request has completed. If you have installed TIBCO MFT Internet Server, you can execute an TIBCO MFT Internet Server Command Line Utility command as a PPA.

The advantage of doing this is that you can perform a file transfer and then execute for instance, an TIBCO MFT Internet Server Command Line Utility command within a single step. See *TIBCO Managed File Transfer Internet Server Command Line Utilities Guide* for more information about the TIBCO MFT Internet Server Command Line Utilities.

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

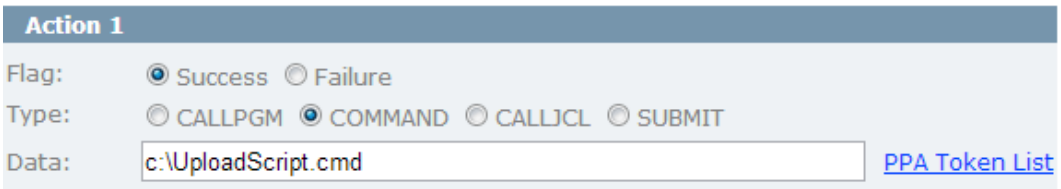
When using PPA to initiate an TIBCO MFT Internet Server Command Line Utility command or any command for that matter, it is good practice to get the command running successfully in batch mode first. For this example, first use the file transfer command for the Internet Server Command Line Client Utility to ensure that the request is executed successfully. After the command is run successfully, you can add it as a PPA request.

Assume that you want to upload a file to Internet Server, and after that file transfer request is completed, you want to launch a script that uses the command line utility to send that file to another MFT server.

You should first ensure that your TIBCO MFT Internet Server Command Line Utility ran successfully from a batch job by testing it; see the following example (the file name is `UploadScript.cmd`):

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

After the command is tested, add the script to a Post Processing Action in your TIBCO MFT Internet Server transfer definition.



After that, each time this transfer request is run, this PPA will start upon the success of the file transfer.

Configuring the Target TIBCO MFT Internet Server System

TIBCO MFT Internet Server comes with a script that will work when you issue Administrator Command Line Client Utility commands. When you want to execute the Administrator Command Line Client Utility command as part of a file transfer request, you must create a new script that is tailored for the environment that you are running.

For information of how to generate the script for Windows and UNIX environments, see the following introductions:

- Configuring the Windows environment
- Configuring the UNIX environment

Configuring the Windows Environment

When you want to execute the Administrator Command Line Client Utility command as part of a file transfer request in the Windows environment, you must create a new script that is tailored for the Windows environment.

When the Administrator Command Line Client Utility (CFAdmin) is installed on Windows, a file called `cfcc.bat` is created.

The following example 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\jre1.6.0_66\bin; ;
call setutilcp
java cfcc.CFAdmin t:%1.xml %2 %3 %4 %5 %6 %7 %8 %9
```

The above script performs the following functions:

- 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.
- 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.
- It sets the `PATH` variable to include the Java JRE (Java Runtime Environment). If the correct JRE is already included in the `PATH` variable, this step can be skipped.
- It calls the `setutilcp.bat` file included with the Administrator Command Line Client Utility. This file sets up environment variables needed by Java to execute.
- The last statement is the actual Java command that executes the Admin Command Line Client Utility. The Admin Command Line Client Utility is named CFAdmin. 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`** - **`%9`** support you to override up to 8 parameters defined in the template XML file.

On Windows, the Java program name (CFAdmin) is case sensitive.

Configuring the UNIX Environment

When you want to execute the Administrator Command Line Client Utility command as part of a file transfer request in the UNIX environment, you must create a new script that is tailored for the UNIX environment.

When the Administrator Command Line Client Utility (CFAdmin) is installed on a UNIX computer, a file called `cfcc.sh` is created.

The following example 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:xerce
sImpl.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:

- The first line (`#!/usr/bin/ksh`) is required and defines the UNIX system to use the korn shell to execute this procedure.
- 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.
- The export PATH statement updates the `PATH` variable to include the JRE (Java Runtime Environment) executables . If the default path includes this directory, this step is not needed.
- 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.
- The last statement is the actual Java command that executes the Administrator Command Line Client Utility. The Administrator Command Line Client Utility is named CFAdmin. 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`** - **`%9`** support you to override up to 8 parameters defined in the template XML file.

On UNIX, the Java program name (CFAdmin) is case sensitive.

Template Users

The following users are automatically added as template users to the database during the TIBCO 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.

Template Users

User ID	Right
admin	AdministratorRight TransferRight
HelpDeskUser	HelpDeskRight UpdateSessionRight ViewAlertRight ViewAuditRight ViewUserRight
TransferUser	TransferRight

User ID	Right
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 enabled. There are no rights given to the collector ID.

Applet Wrapper

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

See Class Parameters for more information on how to use the applet wrapper.

Required Concepts

Before you can use the applet wrapper to transfer a file, you should understand the following concept and working flow used by TIBCO MFT Internet Server.

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

File Record

A transfer definition is a record in the TIBCO MFT Internet Server database that represents a user's ability to transfer one or more files. You can view all properties of a transfer definition using the web interface or the command line utility (the Platform Transfer Client Utility reveals less information than the Administrator Client Utility). The important properties for file transfer are as follows:

Property	Description
FileId	This property must be used to set the **fileID** value of the applet wrapper.
SendRecvFlag	This is a flag which indicates the transfer direction. The **transferDirection** parameter of the applet wrapper must be set according to this value. The valid values are as follows: • S: SEND • R: RECEIVE

Property	Description
CompressType	This is a flag which is used to indicate whether the transfer is compressed. The **compression** parameter of the applet wrapper must be set according to this value. The valid values are as follows: • `0`: NO • `1`: YES
ChkptRestartFlag	This is a flag which indicates whether checkpoint restart is enabled for the transfer. The **restartTransfer** parameter of the applet wrapper must be set according to this value. The valid values are as follows: • `0`: NO • `1`: YES
ChkptInterval	This property specifies the checkpoint interval in seconds. The **checkpointInterval** parameter of the applet wrapper must be set according to this value. The value in file record is in minutes. If you set the**checkpointInterval** parameter according the value in file record, you must convert the value in minutes to a value in seconds by multiplying by 60.
DirectoryTransfer	This is a flag to indicate whether the transfer is a directory transfer. The applet wrapper acts differently for a directory transfer. For more details on directory transfers, see . The valid values are as follows: • `1`: directory transfer. • `0`: not a directory transfer.

Directory Transfer

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

Before any file transfer, the user must know whether the transfer is a file transfer or a directory transfer by selecting `DirectoryTransfer` in the file record. If it is a file transfer, set the necessary parameters of the applet wrapper (see the section of Class Parameters) and perform the transfer. Generally speaking, your transfer definitions should be defined as directory transfers unless there is a specific use case for an individual file transfer. If it is a directory transfer, it contains the following two situations:

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

Directory File List

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

Major part of source code of this class (extracted from the `FTClient.jar` file) is as follows:

```
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 value of the **`elementType`** parameter is `F`, this element is the leaf node and the **`elementName`** parameter is a server file name. If the values of the **`elementType parameter`** is `D`, this element is a subdirectory and you should go into the directory, maybe recursively, to find the file name.

Using the Applet Wrapper

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

Prerequisites

The SIFTSingleFileTransfer class is in `NonGUIApplet_0.0.0.1.jar` file which will be in the directory after installing the TIBCO MFT Internet Server File Transfer Command Line Utility. Put the `NonGUIApplet_0.0.0.1.jar` file in your **classpath** when compiling and running your application.

Procedure

1. Test the file record, for example, through SOAP calls, to get necessary information about a file to set some parameters of the applet wrapper.
2. Set the class parameters of the applet wrapper using set methods.
   See Class Parameters for detailed descriptions of the class parameters.
3. call the transferSingleFile() method to transfer the file.

What to do next

After the file transfer is completed, you can use the Get Result class to get information of the transfer.

The following information are returned:

- **returnCode**: the return code from the applet.
- **bytesTransfered**: the number of bytes transferred.
- **compressedByte**: the number of compressed bytes transferred.
- **returnMsg**: the return message from the server.

Class Parameters

The following table lists the class parameters that must be set using set methods:

Parameter	Description
`fileTransferServletURL`	The 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 defines that the applet is sending or receiving. The value of `SEND` indicates that the applet is sending. The value of `RECEIVE` indicates that the applet is receiving. The parameter must be set based on the value in the file record. The default value is `RECEIVE`.
`fileID`	The file ID of the transfer record to be transferred. This parameter must be the same as what is in the file record.
`localFileName`	The path and name of local file to be transferred. This parameter is required.
`serverFileName`	The name of server file to be downloaded for a directory transfer. Only to be used when receiving a file from a directory file record.
`sessionID`	The ID of the current session. This parameter is required. Got the value from previous SOAP call of getSession().

Parameter	Description
compression	This parameter defines whether the compression is used The value of YES indicates that the compression is used. The value of NO indicates that the compression is not used. The default value is YES. Must set this parameter based on the value in the file record.
traceLevel	The level of trace to use. This parameter is optional.
user id	The user ID to be used in an HTTP request requiring the BASIC authentication. This parameter is required.
password	The password to be used in an HTTP request requiring the BASIC authentication. This parameter is required.
restartTransfer	This parameter defines whether the transfer is to be restarted. The value of YES indicates that transfer is to be restarted. The value of NO indicates that transfer is not to be restarted. The default value is NO. This parameter is optional. If it is set, must be based on the value in the file record.
checkpointInterval	The interval in seconds between checkpoints. This parameter is required. if transfer is to be restarted.
synchronize	The value of YES indicates that multiple instantiated applets are to wait to perform transfer one at a time. The value of NO indicates that all applets are to perform the transfer at the earliest chance. The default value is YES. This parameter is optional.

File Transfer Examples

You can refer to the following examples to configure the SIFTSingleFileTransfer class for transferring a file.

Uploading a file to a 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();
```

Downloading a file from a 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
```

Directory Transfers

TIBCO MFT Internet Server has the ability to transfer directories and subdirectories using one transfer definition in the TIBCO MFT Internet Server File Transfer Command Line Utility.

You should be careful when defining directory transfers because the way that uploads and downloads are handled vary.

When adding a transfer definition, click **Directory Transfer** if you want to define a directory transfer. File tokens can be used, but only in the **Server File Name** field (and only for Uploads). See Add Transfer for details about how to add an Internet transfer definition to TIBCO MFT Internet Server.

Directory Transfers using TIBCO MFT Internet Server Platform Command Line Utility

Executing a directory transfer on the command line works the same way as doing a single file transfer, except that extra commands 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**

Two additional parameters need also be used:

Parameter	Description
SubDir	Defines whether TIBCO MFT Internet Server scans subdirectories for files to transfer in directory uploads, and defines whether TIBCO MFT Internet Server processes data in TIBCO MFT Internet Server server subdirectories for directory downloads. When `No` is specified, TIBCO MFT Internet Server only processes files in the defined directory. When `Yes` is defined, TIBCO MFT Internet Server processes files in the subdirectories and in the defined directory. This parameter is valid only for TIBCO 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	Defines a single server file name to download. This parameter is used only on directory download requests. It is only supported on **ListFile** and **ProcessFile** calls.

Processing for a Download Directory

You can specify the following three parameters to configure the process for a download directory.

Parameter	Description
LocalFileName	Defines a directory or a file name.
FileName	Defines the server file name of TIBCO MFT Internet Server.
SubDir	Defines whether to process files in subdirectories.

When the **FileName** parameter is defined, it means that you want to process only a single file. If the **FileName** parameter does not point to a valid server file name of TIBCO MFT Internet Server, the request fails. If the **LocalFileName** parameter is not defined, TIBCO MFT Internet Server stores the file in the directory pointed to by the **ClientFileName** parameter of the TIBCO MFT Internet Server server. If the **LocalFileName** parameter points to a file, the file is saved to that file name. If the **LocalFileName** parameter points to a directory, the file is saved to that directory using the name defined by the **FileName** parameter. If the **LocalFileName** parameter is not defined as either a file or directory, it is treated as a file name. If the fully qualified file name is invalid, the request will fail, and no directory is created in this case.

When the **FileName** parameter is not defined, it means that you want to process the contents of the directory. If the **LocalFileName** parameter is not defined, TIBCO MFT Internet Server stores the files in the directory pointed to by the **ClientFileName** parameter of the TIBCO MFT Internet Server server. If the **LocalFileName** parameter points to a directory, the files are saved to that directory using the names of the server files. If the **LocalFileName** parameter does not point to a directory, an error is displayed. TIBCO MFT Internet Server does not create the high-level directory; the high-level directory must exist. If the **SubDir** parameter defines to process subdirectories, subdirectories should be created within the directory pointed to by the **LocalFileName** parameter (or the **ClientFileName** parameter if the **LocalFileName** parameter is not defined).

Processing for an Upload Directory

You can specify the following two parameters to configure the process for an upload directory.

Parameter	Description
`LocalFileName`	Defines a directory or a file name.
`SubDir`	Defines whether to scan subdirectories for files.

When the **`LocalFileName`** parameter points to a file, then TIBCO MFT Internet Server transmits that file only. When the **`LocalFileName`** parameter points to a directory, then TIBCO MFT Internet Server transmits all files within the directory.

Email Processing

You can configure TIBCO MFT Internet Server to send emails from a variety of pages and forward the emails to the defined server.

Email notification occurs in the following situations:

- 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, emails can be sent to all users within the group.
- When a file transfer is completed, either successfully or unsuccessfully, email can be sent to different email addresses based on whether the transfer is successful or unsuccessful. For example, you can send an email to the accounting department when a transfer is successful, and send an email to the help desk when a transfer fails. Email can also be sent for Internet Server transfers and Platform Server transfers and can have multiple recipient addresses separated by a comma.
- Email can also be sent for the Platform Server to Platform Server transfers. They will be sent via the initiating TIBCO MFT Platform Server system and will not use the templates defined in TIBCO MFT Command Center or TIBCO MFT Internet Server.

TIBCO MFT Internet Server email can be configured to change the look and feel so that the emails are in any format that you want. TIBCO MFT Internet Server email templates are built using XML. They are simply files on the TIBCO MFT Internet Server server and can be changed using any text editor. No restriction is set to the number of email templates that you can define. The email templates can be customized for individual users and companies. TIBCO MFT Internet Server provides four different email templates. See Email Templates for detailed information of the four email templates.

To implement the email capability, you must configure the system to define when emails must be sent. See Configuring TIBCO MFT Internet Server for Email Support for information of how to configure TIBCO MFT Internet Server for email support.

See the following introductions for how to configure email notification for each situation:

- Configuring Email Notification for Transfer Availability
- Configuring Email Notification for File Transfer Completion

Configuring Email Support

To support email notification, you must configure the TIBCO MFT Internet Server server email parameters in the Global Settings section on the System Configuration page which can be accessed by clicking **Administration** > **System Configuration**.

The following table lists the parameters for email support:

Parameter	Description
Email Admin User Id	Defines the administrator user ID for the email server. This is an optional field. It is only required when the email server requires a user ID and password.
Email Admin User Pwd	Defines the administrator password for the email server. This is an optional field. It is only required when the email server requires a user ID and password for authentication.
Email Failure Template	Defines the default value for the **Email Failure Template** parameter. This is an optional field. This definition can be overridden by the **Email Failure Template** parameter defined in the Internet transfer definition. If a template is defined here, instead of in the Internet transfer definition, 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 TIBCO 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	Defines the name of the email system; for example, `emailserver.company.com`. This parameter is required if you want to use the email features. If this field is not defined, TIBCO MFT Internet Server email support is disabled.  Although this field can contain an IP address, it typically contains the IP name of the email server at your site.
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`.
Email Success Template	Defines the default value for the **Email Success Template** parameter. This is an optional field This template can be overridden by the **Email Success Template** parameter defined in the Internet transfer definition. If a template is defined here, instead of in the Internet transfer definition, 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 MFTCC `email-template` directory, you can enter the file name. Otherwise, you must enter the fully qualified file name including the path.
SMTP TLS	Defines if SSL/TLS is used for the SMTP connection.
Trust SMTP SSL Certificates	Defines whether TLS/SSL SMTP certificates is to be trusted.

Configuring Email Notification for Transfer Availability

When a file is added to the system, email can be sent to all users configured to perform transfer of the file.

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

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

Procedure

1. Define the email address within the TIBCO MFT Internet Server user record for the user associated with the transfer request.

   If no email address is defined in the user record, no file availability notification email will be sent to that user.

2. When a transfer record is added for a user or group of users, define the **File Notification Email Template** field with a valid email template file name.

   The name must exactly match the name of the template file. When processing an email template, TIBCO MFT Internet Server first looks in the TIBCO MFT Internet Server server `/cfcc.war/email-template` directory for the email template file specified. If you do not specify a fully qualified name, 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, you have to define the fully qualified email template file name in the **File Notification Email Template** field.

Configuring Email Notification for File Transfer Completion

You can configure TIBCO MFT Internet Server server to send email notification messages to authorized users upon transfer completion.

You can send transfer completion messages on success and failure. You can send the success and failure emails to different email addresses.

To use this support, the **Email Success Template** and **Email Failure Template** parameters must be defined and the target email addresses must be defined.

To implement transfer completion email notification, perform the following steps:

Procedure

1. Define the email template files.

   You can define the email template file either through the **Administration** > **System Configuration** options or through the **Transfer** option.

   If the template is defined in both places, the Internet Server transfer definition overrides the TIBCO 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 **Success Recipient** and **Failure Recipient** fields in the Email Notification section in the Internet Server transfer definition. 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.

What to do next

After the configuration parameters are defined, you can run a transfer. If the transfer is successful, the email will be sent to the email address of the user defined by the **Success Recipient** field.

Completion email notification is sent only if the file transfer was actually started. If an error occurs before the transfer is started, no email will be sent.

Email Templates

TIBCO MFT Internet Server provides four different email templates built using XML. You can edit the email templates using any text editor.

TIBCO MFT Internet Server provides the following email templates:

- File Availability Template
- Transfer Completion Templates

The two types of templates are configured differently and use different XML DTD files. You can change the format of the template XML files, but you cannot update the DTD files. The XML files includes references 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 TIBCO MFT Internet Server server `email-template` directory), the DTD files should be copied from the `email-template` directory into the directory where the XML files are located.

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 has a value of either `UPLOAD` or `DOWNLOAD`.

File Availability Template

TIBCO MFT Internet Server provides a file availability template. The template is named as `email-notification-template.xml` and is located by default in the `<MFT_Install>\server\webapps\cfcc\email-template` directory.

The following example is a copy of the file availability template that is shipped with the TIBCO MFT Internet Server software:

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

<!-- Sample file notification template  -->

<file-notification-email>
    <sender>
        <address><token name="emailsender"/></address>
    </sender>
    <subject>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:
        <token name="emailurl"/>/bclient/index.jsp?FileID=<token name="fileid"/>
        To check for all available files, click on the following URL:
        <token name="emailurl"/>/bclient/index.jsp

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

The following table lists the description for each line in the template:

Line	Description
`<!DOCTYPE file-notification-email SYSTEM "file-notification-email.dtd">`	This line defines the DTD file associated with the XML file. You 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>`
`</sender>`
	This line defines the name of the email sender.
	The default sender name is `emailsender`.
	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).
	  Some email systems require this to be a valid email address.

`<subject>File Availability Notification</subject>`	This line 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:` `<token name="emailurl"/>/bclient/index.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. When you click the URL, you will be brought directly to the screen where you can access the file.  The administrators must change the field `host:port` to point to their TIBCO MFT Internet Server server. If you build your own user interface, you can insert the URL to your page here as well.
`To check for all available files, click on the following URL:` `<token name="emailurl"/>/bclient/index.jsp`	These fields define the URL that can be used to access all transfer definitions that are available for you. When you click the URL, you are brought directly to the screen where you can start the TIBCO MFT Internet Server file transfer applet.  The administrators must change the field `host:port` to point to their TIBCO MFT Internet Server server. If you build your own user interface, you can insert the URL to your page here as well.

Tokens Supported in the File Availability Template

You can use tokens in the file availability template provided by TIBCO MFT Internet Server.

The format of a token is as follows:

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

Where, *xxxxxxxxxx* defines the name of the token. The following tokens are supported in the file availability template:

Token	Description
fileid	This token is typically used in the URL to define the file name that has just been made available.
clientfilename	This token defines the name that has been defined for the file on the client side.
serverfilename	This token 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, it is good practice to not add 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 token defines the description that was defined for the file in the transfer record. This is an important field for the client because it can describe the contents of the file to be sent or received.
availabledate	This token defines the date that the file will be made available to transfer.
expirationdate	This token defines the date that the file will expire and be no longer valid for transfer.
transferdirection	This token defines whether the transfer will be an upload (client to TIBCO MFT Internet Server server) or a download (TIBCO MFT Internet Server server to client).

Transfer Completion Templates

TIBCO MFT Internet Server provides two file transfer completion templates: one for successful transfers and one for unsuccessful transfers. The templates are named as `transfer-success-email-template.xml` and `transfer-failure-email-template.xml` and are located by default in the `<MFT_Install>\server\webapps\cfcc\email-template` directory.

The following example is a copy of the transfer completion template for successful transfers.

The two templates are essentially the same except for some comments indicating the success or failure of the transfer.

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

<!-- Sample file notification template -->

<file-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="transfer direction"/>
                Client File Name: <token name="client filename"/>
                To Server: <token name="node"/>
                Server File Name: <token name="server filename"/>
                Start Time: <token name="stardom"/>
                End Time: <token name="endtime"/>
                Byte Count: <token name="betokened"/>
                Transfer Status: <token name="transferstatusmsg"/>
                Audit ID: <token name="auditid"/>
                Client IP: <token name="clientip"/>

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

The following table lists the description for each line in the template:

Line	Description
`<!DOCTYPE file-notification-email SYSTEM "file-notification-email.dtd">`	This line defines the DTD file associated with the XML file. You 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 in the **Sender Email Address** field in the Global Settings section on the System Configuration page. This email address can be changed to any appropriate email address. When the user receives an email from TIBCO MFT Internet Server, the data entered here will be shown as the Sender (or From).

Line	Description

`<recipient>`
`<address><token name="recipientemailaddress"/>`
`</address>`
	This code is currently commented out. It defines the default recipient.
	If you define an email address in the **Success Recipient** field of a transfer definition, this user will receive an email when a transfer is conducted successfully. If no email address is defined here, no email will be sent.
	If you want 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"/>`, add a recipient email address, such as, `user@xyzcompany.com`. One reason you might want to do this is for a specific user to get all the emails when a transfer fails. This can be a technical support user in your company. To do this, set the user ID in the `transfer-failure-email-template.xml` file. That way, an email will be sent to that user when any requests fail.

`<subject>File Transfer Success Notification</subject>`	This line 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 also insert other comments or instructions here.

`User: <token name="user id"/>`
`Transfer Direction: <token name="transfer direction"/>`
`Client File Name: <token name="client filename"/>`
`To Server: <token name="node"/>`
`Server File Name: <token name="server filename"/>`
`Start Time: <token name="stardom"/>`
`End Time: <token name="endtime"/>`
`Byte Count: <token name="betokened"/>`
`Transfer Status: <token name="transferstatusmsg"/>`
`Audit ID: <token name="auditid"/>`
`Client IP: <token name="clientip"/>`
	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 is substituted for the token.

Tokens Supported in Transfer Completion Templates

You can use tokens in the transfer completion template provided by TIBCO MFT Internet Server.

The format of a token is as follows:

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

Where, *xxxxxxxxxx* defines the name of the token. The following tokens are supported in the file availability template:

Token	Description
auditid	This token defines the audit record number associated with the file transfer request. This token 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 token 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 token defines the name that has been defined for the file on the client side.
endtime	This token defines the time when the file transfer request was completed.
fileid	This token is typically used in the URL to define the record ID of the file that was transferred.
node	This token defines the target server associated with the file transfer.
proxystatusmsg	This token 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 token 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 token defines the session ID used for the file transfer. This is for information purposes only.
starttime	This token defines the time when the file transfer request was started.
transferdirection	This token defines whether the transfer will be an upload (client to TIBCO MFT Internet Server server) or a download (TIBCO MFT Internet Server server to client).
transferstatus	This token defines the transfer status. It can be `SUCCESS` or `FAILURE`.
transferstatusmsg	This token defines the last message associated with the file transfer request. This is often a generic message that indicates that the transfer failed.
userid	This token defines the user ID associated with the file transfer.

File Tokens

TIBCO MFT Internet Server supports the use of file tokens in the server file name.

When creating a file record in the TIBCO 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)*

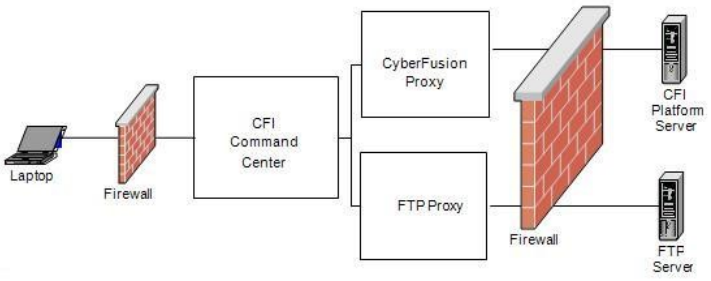
If tokens are available, you can click **File Token List** next to the **Server File Name** field on the Add Transfer page for the complete token list.

FTP Proxy

TIBCO MFT Internet Server does not require any third party software to send to a remote system that is something other than the TIBCO MFT Internet Server. TIBCO MFT Internet Server has been enhanced with the capability to proxy TIBCO MFT Internet Server file transfers to FTP servers.

This converts HTTP data to FTP protocol in order to send data to an FTP server. This enables an TIBCO MFT Internet Server client to access data on many computers (nodes) within a customer site. Because almost all organizations have access to an FTP or Secure FTP server, this also allows TIBCO MFT Internet Server to push files to the client FTP servers.

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



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

- File data to be transferred to/from the client does not have to reside on the Internet Server 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 TIBCO MFT Platform Server directory proxy.

To configure TIBCO MFT Internet Server to proxy to an FTP server, create a node with the parameters listed in the following table, and then, create a file record and specify the newly created node for the `Node Name` parameter.

Parameter	Description
`Node Name`	The name of node.

Parameter	Description
IP Name	The IP name/address of the FTP server.
IP Port	The port number that the FTP server is listening for connections.
Node Type	The node type is FTP.
Server Type	The operating system of the FTP server (or operating system that the FTP server is emulating)
Data Connection Type	The data connection type. The following types are available: • PORT: often referred to as Active FTP. When Active FTP is used, the FTP server establishes the data connection back to the FTP client. When an FTP data connection is required, the FTP client sends the **PORT** command to the FTP server to tell the FTP server how to establish a connection back to the FTP client. PORT is the default type. • PASV: often referred to as Passive FTP. When Passive FTP is used, the FTP client establishes the data connection to the FTP server. When an FTP data connection is required, the FTP client sends the **PASV** command to the FTP server. The FTP server then responds with a **PORT** command to tell the FTP client how to establish a data connection to the FTP server. • EPRT: an extended version of the **PORT** command. When EPRT is used, the FTP server establishes the data connection back to the FTP client. When an FTP data connection is required, the FTP client sends the **EPRT** command to the FTP server to tell the FTP server how to establish a connection back to the FTP client. • EPSV: an extended version of the **PASV** command. Its main advantage is that it does not return an IP address in the response to the FTP client. When EPSV is used, the FTP client establishes the data connection to the FTP server. When an FTP data connection is required, the FTP client sends the **EPSV** command to the FTP server. The FTP server then responds with an **EPSV** command to tell the FTP client how to establish a data connection to the FTP server.  You need to configure this parameter when the FTP Proxy component is having trouble transferring though a firewall.
Connection Security Type	The connection security type when proxying to an FTP server. The following types are available: • 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.

FTP Server

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

The TIBCO MFT Internet Server FTP server has the following features:

- RFC 959 Compliance
- RFC 2228 Compliance for FTP over SSL (Explicit SSL Support)
- Implicit SSL Support

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

TIBCO 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

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

A TIBCO MFT Internet Server transfer definition is mapped to 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 example, 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 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 user's VDS. The user would see the `data.txt` file in their root directory.

Example

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

Assume that there is a directory, `c:\test1`(Client File Name), on the client's side containing the `file1.txt` and `file2.txt` files. The client will perform an FTP Upload (put) and an FTP Download (get) to and from the TIBCO MFT Internet Server FTP Server on 192.168.333.333. There is a directory, `c:\test2`, on the TIBCO MFT Internet Server server (server file name) that contains the `file3.txt` and `file4.txt` file. The transfer is done using the user ID, user1.

Two file definitions should be created for the user1 user to perform these FTP transactions, one for Upload and one for Download. As stated earlier, both files should point to the `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`** parameter will be set to `/FtpFiles`.

1. The user1 user performs an FTP login from the client side `c:\test1` directory onto the TIBCO MFT Internet Server FTP server on 192.168.333.333. The `Welcome!` message configured on the TIBCO MFT Internet Server server is displayed.

```
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.
```

2. The user1 user 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
```

The FTPFiles directory is an FTP File Alias parameter value which corresponds to the `c:\test2` server directory.

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 the user1 user 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.

3. The user1 user performs listing of `/FtpFiles` directory 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
```

4. The user1 user performs an Upload (put) of the `file1.txt` file 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
```

5. The user1 user performs Download (get) of the `file3.txt` file 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.
```

Multi-Language Support

TIBCO MFT Internet Server supports multiple languages for various file transfer clients of TIBCO MFT Internet Server. 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.

The multi-language support is applied in TIBCO MFT Internet Server as follows:

- All messages and text that are displayed to the end user using the MFT file transfer web page is displayed in the language preferred by that end-user. The TIBCO MFT Internet Server administration web pages do not support multiple languages and are shown in English.
- All dates and times that are displayed to the end user performing the file transfer are displayed in the format preferred by that end user's region (according to language). The TIBCO MFT Internet Server administration web pages are to be provided in the U.S. format only.
- File transfer end-user messages consist of text produced by the following TIBCO MFT Internet Server components:

  - File transfer applets: includes the Java client file transfer applet as well as the file browse applet.
  - File transfer web pages: includes the web pages that support the Java 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 remain in English.
- File transfer end users communicate in their preferred language to TIBCO MFT Internet Server by configuring their browser and local operating system to request information in their preferred language.

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 TIBCO MFT Internet Server, all messages and text will be in English.
- TIBCO MFT Internet Server supports the following languages: English, French, Italian, Portuguese, Spanish.
- Multiple language support is performed on the machine that produces the text to be translated. In other words, language translation for JSPs and Servlets occurs on TIBCO MFT Internet Server, while language translation for applets and the TIBCO MFT Internet Server File Transfer Command Line Utility occurs on the client machine.

Changing the User ID or Password of the Database

You can use the **`dbsettings`** utility to change the user ID/password of the database defined in your web server's `web.xml` file. The utility can save the database password in an encrypted format if you want.

To do this, run the `dbsettings.bat` script for Windows (dbsettings.sh for UNIX) in the *`<MFTIS_Install>`*`\distribution\util\dbsettings` directory.

The following figure shows an example:

```
* 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.
```

When 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 want.

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, choose option 2 and enter the new database URL, for example, **`jdbc:jtds:sqlserver://10.1.2.182:1433/MFT67;domain=DomainName`**.

Sample JMS XML

TIBCO MFT Internet Server and TIBCO MFT Command Center have 9 JMS XML schema files ending with the `.xsd` extension and 3 accompanying sample XML files.

To view any of the XML schema or sample files, it is good practice to use a text editor, such as Notepad or NotePad++.

Using JMS XML files

Each XML file has a corresponding XSD file. We have provided three sample XML files. When you want to create an accompanying XML file for one of the XSD files, see the element details in the XSD files.

JMS XML Schema and XML files

The XSD file defines the rules that must be followed when creating XML files and therefore should not be updated. The XML file defines the parameters necessary to perform a JMS function.

When you want to update the XML files, it is good practice to copy them to a new folder to keep the original files in their original status. Each sample XML file has a corresponding XSD file. See the XSD file associated with the XML file for the rules that define allowable values in the XML file.

All XSD and sample XML files can be found in the *<MFTIS_Install>*`/server/webapps/`*<context>*`/example/JMS` directory.

XSD Files

XML Schema File	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. This XSD file is used for multiple responses and returns an array of 0 or more audit records. For the 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 TIBCO MFT Command Center and TIBCO MFT 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 management request is initiated and the request type is `ManageConfigRequest`. This response XML maps the MFT JMS configuration parameters.

XML Schema File	Description
`ManageRequest.xsd`	Defines the format of the parameters necessary to initiate a management request. This request is used internally to extract configuration information from TIBCO MFT Internet Server. Three request types are allowed: • ManageConfigRequest: returns the JMS configuration parameters. • ManageServerRequest: returns a list of MFT servers defined to TIBCO MFT Internet Server. • ManageServerTransfers: returns a list of pre-defined transfers.  The ManageServerRequest request will return a different list of servers based on the request JMS type set: • ManageServerRequest: returns all Platform Server servers. • ManageServerRequestIS: returns all Internet Server servers.
`ManageServerResponse.xsd`	Defines the XML data that is returned when a management request is initiated and the request type is ManageServerRequest. There are two types of responses that can be returned, based on the JMS type setting of the ManageServerRequest request: • ManageServerRequest: returns the name of all Platform Server servers defined to TIBCO MFT Internet Server. • ManageServerRequestIS: returns the name of all Internet Server servers defined to TIBCO MFT Internet Server.
`ManageTransferResponse.xsd`	Defines the XML data that is returned when a management request is initiated, the request type is ManageTransferRequest and the request JMS type is ManageTransferRequest. This response returns all Platform Server transfers defined to TIBCO MFT Internet Server.
`ManageTransferResponseIS.xsd`	Defines the XML data that is returned when a management request is initiated, the request type is ManageTransferRequestIS and the request JMS type is ManageTransferRequestIS. This response returns the all Internet Server transfers defined to TIBCO MFT Internet Server that the user defined in the ManageRequest request is authorized to access.

XML Schema File	Description
`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. Two JMS records can be returned for this request: • Immediate response: indicates whether the request has been accepted and submitted to Internet Server for processing. This response does not have XSD data 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`.
`TransferRequestPlatformServer.xsd`	Defines the format of the parameters required to initiate a Platform Server transfer. This is occasionally called a 3rd party transfer. TIBCO MFT Internet Server retrieves data from the JMS queue and initiates a transfer to the Platform Server A to transfer a file to/from the Platform Server B. Two JMS records can be returned for this request: • Immediate response: indicates whether the request has been accepted and submitted to the Platform Server server for processing. This response does not have XSD data 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`.
`ExecuteJobRequest.xsd`	Defines the format of the parameters necessary to initiate the execution of a scheduler job.
`ExecuteJobResponse.xsd`	Defines the XML data that is returned when the execution of a scheduler job is initiated. This response returns "0" or "Success" if the request is successful, or it returns the details of the error message if the request fails.

XML Files

Sample XML File	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`	Defines sample XML data to initiate a Platform Server transfer.  This sample file is used for TIBCO MFT Command Center requests only.
`ExecuteJobRequest.xml`	Defines sample XML data to initiate the execution of a Scheduler job.
`ExecuteJobResponse.xml`	Defines sample XML data to return when the execution of a Scheduler job is initiated.

ID Information

TIBCO MFT 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 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.

The following table lists the components of an ID:

Byte	Description
1	The source of the ID: • A: TIBCO MFT Platform Server Internet audit • C: TIBCO 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	The month: • 1: January • 2: February • 3: March • 4: April • 5: May • 6: June • 7: July • 8: August • 9: September • A: October • B: November • C: December
3,4	The day of the month from 01 to 31.
5	The year. F-2015 through Z-2036

Byte	Description
6-12	The sequential number in hex between 0 to FFFFFFF.

Appendix A. Configuring the RADIUS Authentication

MFT supports authentication to a RADIUS server. This can be used to provide multi-factor authentication using tokens or security cards. You can configure RADIUS authentication through the `web.xml` file.

When configured, RADIUS authentication will replace all user ID and password authentications for the MFT instance, except for users configured in the RADIUS-SpecialUsers parameter in the `web.xml` file.

To configure RADIUS configuration, perform the following steps:

1. Updating the Trace Settings
2. Defining RADIUS Configuration Parameters
3. Setting the RADIUS Primary and Backup Secrets
4. Restarting the MFT Server

Updating the Trace Settings

To configure RADIUS authentication, you must first update the trace settings.

Edit the following file:

```
<MFT Install>\server\webapps\cfcc\WEB-INF\classes\log4j.properties
```

If the following RADIUS entries listed are not in the `log4j.properties` file, add these lines to this file. The placement of these lines is not important as long as it is not in the middle of another section.

```
# Set logging level for RADIUS authentication
log4j.logger.com.proginet.sift.login.RADIUSAuthMethod=TRACE, RADIUSFile
log4j.appender.RADIUSFile.File=${cfi.trace.dir}/RADIUS-trace.txt
log4j.appender=org.apache.log4j.DailyRollingFileAppender
log4j.appender.RADIUSFile.ImmediateFlush=true
log4j.appender.RADIUSFile.Append=true
log4j.appender.RADIUSFile.DatePattern='-'yyyy-MM-dd
log4j.appender.RADIUSFile.layout=org.apache.log4j.PatternLayout
log4j.appender.RADIUSFile.layout.ConversionPattern=%d{dd MMM yyyy HH:mm:ss} [%t] %-5p
%c - %m%n
```

Normally the trace level is set to `ERROR`. It is good practice to set the trace level to `TRACE` while configuring and testing RADIUS for the first time. After RADIUS has been tested, set the trace level to `ERROR`.

For these changes to take place, the MFT server must be restarted.

Defining RADIUS Configuration Parameters

After updating the trace settings, you have to define RADIUS configuration parameters in the `web.xml` file.

The `web.xml` file is typically located in the `<MFT Install>/server/webapps/cfcc/WEB-INF/web.xml` directory. To configure RADIUS authentication, you must add the following parameters to the `web.xml` file. These parameters should be placed with the other **`context-param`** parameters before the **`filter`** parameters.

See Sample web.xml RADIUS Parameters for sample RADIUS `web.xml` parameters.

Web.xml Parameter	Description
RADIUS-Enabled	Defines whether RADIUS authentication is enabled or disabled. The valid values are as follows: • `True`: RADIUS authentication is enabled and will replace MFT user ID and password authentication. • `False`: RADIUS authentication is disabled. Standard MFT user ID and password authentication will be used. This is the default value.
RADIUS-PrimarySecret	Defines the primary RADIUS encrypted secret.  This parameter is set by executing the **dbsettings** utility and must be set before performing RADIUS authentication. It cannot be set manually.
RADIUS-PrimaryHost	Defines the IP address or IP name of the primary RADIUS server. This parameter is required if RADIUS authentication is enabled.
RADIUS-PrimaryPort	Defines the IP port of the primary RADIUS server. This parameter is required if RADIUS authentication is enabled.
RADIUS-PrimaryAdapterIP	Defines the IP address that will be used when communicating with the primary RADIUS server. The default value of `0.0.0.0` indicates accepting responses over any adapter.
RADIUS-BackupSecret	Defines the backup RADIUS encrypted secret. This parameter is required only if you want to communicate to a backup RADIUS server.  This parameter is set by executing the **dbsettings** utility and must be set before performing RADIUS authentication. It cannot be set manually.
RADIUS-BackupHost	Defines the IP address or IP name of the backup RADIUS server. This parameter is required only if you want to communicate to a backup RADIUS server.
RADIUS-BackupPort	Defines the IP port of the backup RADIUS server. This parameter is required only if you want to communicate to a backup RADIUS server.
RADIUS-BackupAdapterIP	Defines the IP address that will be used when communicating with the backup RADIUS server. The default value of `0.0.0.0` indicates accepting responses over any adapter.

Web.xml Parameter	Description
RADIUS-Synchronous	Defines whether communication to primary and backup RADIUS servers is synchronous or asynchronous. The valid values are as follows: • `True`: RADIUS authentication is synchronous. Communication to the RADIUS backup host will only be performed if communication to the RADIUS primary host times out. • `False`: RADIUS authentication is asynchronous. Requests will be made to both RADIUS primary host and RADIUS backup host at the same time. MFT will use the first response that is received. This parameter is ignored if a RADIUS backup server is not defined.
RADIUS-Timeout	Defines the number of seconds the RADIUS client will wait for a response from the RADIUS server before the request times out and fails.
RADIUS-SpecialUsers	Defines the users that will be authenticated using standard MFT authentication in the event that RADIUS authentication fails. You can define one or more MFT users separated by a semicolon.

Sample web.xml RADIUS Parameters

To configure RADIUS authentication, you have to define RADIUS configuration parameters in the `web.xml` file.

The following example shows sample `web.xml` RADIUS parameters:

```
<!-- Begin RADIUS Parameters -->
        <context-param>
                <param-name>RADIUS-Enabled</param-name>
                <param-value>True</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-PrimarySecret</param-name>
                <param-value> </param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-PrimaryHost</param-name>
                <param-value>10.1.2.100</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-PrimaryPort</param-name>
                <param-value>1812</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-PrimaryAdapterIP</param-name>
                <param-value>0.0.0.0</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-BackupSecret</param-name>
                <param-value> </param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-BackupHost</param-name>
                <param-value>10.1.2.200</param-value>
```

```
        </context-param>

        <context-param>
                <param-name>RADIUS-BackupPort</param-name>
                <param-value>1812</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-BackupAdapterIP</param-name>
                <param-value>0.0.0.0</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-Synchronous</param-name>
                <param-value>False</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-Timeout</param-name>
                <param-value>10</param-value>
        </context-param>

        <context-param>
                <param-name>RADIUS-SpecialUsers</param-name>
                <param-value>admin;mftuser</param-value>
        </context-param>

        <!-- End RADIUS Parameters -->
```

Setting the RADIUS Primary and Backup Secrets

After defining RADIUS configuration parameters in the `web.xml` file, you must executing the **`dbsettings`** utility to save the RADIUS primary and backup secrets.

To execute this utility, follow the following instructions:

- On UNIX,, navigate to the <*`MFTIS_Install`*>`\distribution\util\dbsettings` directory and run the `dbsettings.sh` file.
- On Windows, navigate to the <*`MFTIS_Install`*>`\distribution\util\dbsettings` directory and run the `dbsettings.bat` file.

Follow the instructions to set the RADIUS primary and backup secret keys.

Restarting the MFT Server

To make the RADIUS authentication configurations take effect, you must restart the MFT server after completing the RADIUS authentication configurations.

Appendix B Web XML Parameters

Most TIBCO MFT Internet Server and TIBCO MFT Command Center parameters are configured on the Adminstrator web pages. But there are some parameters that are infrequently used, or must be configured at server startup that are configured in the `web.xml` file. These parameters are documented in this appendix.

The `web.xml` file is located in the *<MFT_Install>*`/server/webapps/cfcc/WEB-INF` directory.

In most cases, you should not update the web.xml parameters unless instructed to do so by Technical Support.

The web.xml parameters are defined by the context-parm element. The parameter name is defined by the param-name attribute while the parameter value is defined by the param-value attribute.

After updating the `web.xml` file, the MFT server must be restarted for the web.xml changes to take effect.

If MFT detects an xml syntax error, the MFT server will not start. See the `catalina.out` file in the *<MFT_Install>*`/server/logs` directory for details.

The web.xml parameters are broken up by functionality into the following tables:

- Security Parameters

  This table lists the parameters that affect the security of the MFT instance.
- Miscellaneous Parameters

  This table lists the parameters that do not fit into the other categories.
- Connectivity/Protocol Parameters

  This table lists file transfer and file transfer protocol parameters.
- RADIUS Authentication Parameters

  This table lists the parameters associated with the RADIUS authentication.
- OEM Parameters

  This table lists the parameters that change the product names and branding.
- Database Driver Parameters

  This table lists the parameters associated with the JDBC connection.
- Database Pooling Parameters

  This table lists the database pooling parameters.

Security Parameters

Security parameters affect the security of the MFT instance.

The following table lists the security parameters:

Parameter	Default	Description
AllowedReferersAdminJSP	By default, referrer URL checking will not be performed.	This parameter allows you to specify the Referrer URL allowed by MFT. Defining Referrer URLs provides an additional layer of security to MFT. This parameter is used by the administrator JSP pages. You can define multiple URLs. Delimit multiple URLs with a comma.  You should enter the URL for this MFT server.
AllowedReferersForXferNavigation	By default, referrer URL checking will not be performed.	This parameter allows you to specify the Referrer URL allowed by MFT. Defining Referrer URLs provides an additional layer of security to MFT. This parameter is used by the file transfer client. You can define multiple URLs separated by commas.  You should enter the URL for this MFT server.
Anonymous	No default	Defines users that can login in without password validation. Ensure that these users have limited file transfer authorization. More importantly, ensure that these users do not have any administrator rights.
BCFipsMode	`False`	Defines whether MFT is using BouncyCastle FIPS mode. The default value of `False` indicates that MFT is not running in FIPS mode, while `True` indicates that MFT is running in FIPS mode.  This value should never be changed manually. The `fips.bat` and `fips.sh` scripts set this value.
BCProvider	No default	Defines the BouncyCastle security provider. Use the default value unless you are instructed by Tech Support to change this.

Parameter	Default	Description
ChangedPasswordEmailEnabled	No	Defines whether an email is sent to a user when the user changes their password. Valid Values: Yes: Sends an email to the user when a user changes their password No: Does not send an email to the user when a user changes their password
HTTPOnlyCookies	True	If set to true, all cookies created by MFT have the HTTPOnly attribute set. By default, httponly is set for MFT generated cookies. There are a few cookies that do not have HttpOnly set, because the JavaScript requires these cookies. The cookies that do not have HttpOnly set do not contain any privileged or sensitive information.
HTTPSCertAuthField	None	Allows you to override the Certificate field that contains the user ID. By default, MFT matches the certificate against the HTTPS public keys defined for users. The web.xml file has a commented value that shows how to use the "SAN:OtherName:PrincipalName" as the user ID.
InstallAdminService	Set during installation	Defines whether the administrator service is installed on an TIBCO MFT Internet Server instance. If the administrator service is installed, this parameter is set to YES. If you set it to NO, the administrator service requests for this instance will fail. Note: If the administrator service for the TIBCO MFT Internet Server instance is not installed and set to NO by the installer, setting this parameter to YES will be ignored.

Parameter	Default	Description
`LoadBalancerIPAddressList`	No default	For HTTP requests that go through a load balancer, MFT will use the HTTP header "X-Forwarded-For" IP address as the IP address of the incoming request when the actual IP address matches one of the addresses defined by this parameter. You can define multiple Load Balancer IP addresses by separating them with a comma.
`PasswordHashNew`	SHA-256	Defines the hashing algorithm used when a user password is changed or a new user is created. Because this password is a hash, it cannot be decrypted.
`PrivacyPolicyURL`	No default	Defines the URL of the privacy policy link that is added to the footer of each browser page. When no value is defined, the footer will not contain a privacy policy link. When any value is defined, the **View Privacy Policy** link will be displayed on the footer of each page. You can click this link to open a privacy policy page.  MFT does not provide a privacy policy page. You must define a privacy policy page that will be opened by the **View Privacy Policy** link.
`SessionTimeOut`	`30`	Defines the session timeout in minutes for active SFTP connections and FTP control connections. If the connection is inactive for longer than the time defined, the next request will fail. The HTTP timeout is set by the **`SessionTimeOut`** parameter configured in the *<MFT_Install>*`/server/conf/cfcc/xml` directory.
`SmtpTLSEnabled`	`false`	Defines whether SSL/TLS is used when communicating to an SMTP server. `false`: Indicates that SSL/TLS will not be used. `true`: Indicates that the SMTP communication will be performed using SSL.

Parameter	Default	Description
UnsecuredHTTPSupport	NO	Defines whether HTTP requests will be accepted. The default value of NO indicates that HTTP Requests will not be accepted. Specifying YES will allow HTTP requests if an HTTP connector is defined.
SSHSecurityLevel	No default	Controls the SSH security level. Based on this setting, cipher/hash/key is automatically chosen. The valid values are: Weak, Strong, Paranoid. (Any other value can also be specified as this parameter is not set.) If this value is specified, the original settings for **SSHCipherSuite**, **SSHKeyExchange**, **SSHDigestSuite** are ignored. If this value is not specified, there is no change.  This setting is quite strict and many clients might stop working at the Strong or Paranoid level.

Miscellaneous Parameters

Miscellaneous parameters refer to parameters that do not fit into the other categories.

The following table lists the miscellaneous parameters:

Parameter	Default	Description
AlertCheckInterval	60	Defines the interval in seconds between checks to see if the Alert Cache needs to be updated. Valid values are from 1 to 60 seconds, and the default value is 60 seconds. You should change this parameter only if you need to lower the elapsed time between when an alert is added, deleted or updated, and when the alert cache is updated.
AssignViewEmailContentsRight	admin	This parameter is not used.
AuditDir	The directory defined during installation	Defines the directory where MFT audit files are located.

Parameter	Default	Description
CacheTimeStampInitYieldSec	120 seconds plus a random number between 1 - 60 seconds	Defines the amount of time that Internet Server and Command Center waits at startup time before monitoring for cache updates and inactive hosts.
CacheTimeStampIntervalSec	30 seconds	Defines how frequently Internet Server and Command Center check for cache updates. It also defines how frequently Internet Server and Command Center check for inactive hosts. For more information on deleting inactive servers, see the **CacheTimeStampRemoveHostThreshold**.
CacheTimeStampRemoveHostThreshold	20 intervals	Defines how many times an Internet Server or Command Center allows a server to be inactive before removing the host from the database. MFT checks if a server is active based on the **CacheTimeStampIntervalSec** parameter. If a server is inactive for the number of times defined by this parameter, the host is removed from the database. This parameter is used only when the Internet Server or Command Instance is a dynamic Cloud instance started with the COM_TIBCO_MFT_CE_TEMPLATE NAME environment variable.  Only Command Centers or Internet Servers with the administrator service installed check for inactive servers.
DefaultTransferClient	browser	Defines the default transfer client. The value of `browser` indicate the default transfer client is the browser client. It is good practice to use the browser client by default. The value of `java` indicate the default transfer client is the Java client.
EmbeddedServer	`true`	This parameter should always be set to `true`.
ExpiredFilesLog	`./ExpiredFilesLog.txt`	This parameter is not used.

Parameter	Default	Description
HTTPOnlyCookies	`True`	If set to true, all cookies created by MFT will have the HTTPOnly attribute set. By default, httponly is set for MFT generated cookies. There are a few cookies that do NOT have httponly set, because the JavaScript requires these cookies. The cookies that do NOT have httponly set do not contain any privileged or sensitive information.
HostName	The host name defined during installation	Defines the host name that was set during the configuration process. This parameter is used to identify the MFT server in the database tables. This should not be changed without guidance from Technical Support.
HttpSSOCustomizationConfigFile	No default	Defines the HTTP SSO customization file. This should only be used when the server is configured to support SSO. Generally, this parameter is set to the SSO configuration file, `httpssocustomization.xml`.
ISCCFlag	None	Set at installation time and notifies the MFT Cloud Servlet whether this installation is for Internet Server or Command Center. The value of this parameter should not be changed
MaximumFileNumber	`10000`	Defines the maximum number of files to be returned to the browser or Java client for a single directory scan.
MessageDir	The directory defined during installation	Defines the directory where MFT message files are located.
MinimumJREVersion	`1.7.0+`	Defines the minimum JRE version for the Java file transfer applet. If the version is less than this value, the user is prompted to upgrade the Java version.
PCISkipFileName	No default	Defines the name of the PCI file that can be used of if you want to skip "Admin Change" logging for a particular field in an object. Refer to file "PCISkip.xml" for details on how to configure this file.

Parameter	Default	Description
S3ClientConfigFile	No default	Defines the S3 config file name.  Do not change this parameter unless instructed to do so by MFT Technical Support.
SAMLAuthenClassRef	`urn:oasis:names:tc:SAML:2.0:ac:classes:Password`	Allows users to update the **SAMLAuthenClassRef** used in the SAML negotiation.  Only do this if you are using a non-standard SAML Authentication Class Ref and are instructed by MFT Support to change this field.
SAMLComparison	`MINIMUM`	Allows users to update the SAML Comparison method. The default value of `MINIMUM` is suggested. Other supported values are: `EXACT`, `MAXIMUM`, or `BETTER`.  Only change this field if you are instructed to do so by MFT Support.
SAMLNameIDType	`urn:oasis:names:tc:SAML:2.0:nameid-format:transient`	Allows users to update the **SAMLNameIDType** used in the SAML negotiation.  Only do this, if you are using a non-standard SAML name ID type and are instructed by MFT Support to change this field.
SearchAuditAtPageEntry	`true`	Defines whether MFT performs an audit search when the Search Audits page is first configured. The value of `true` indicates that MFT performs an audit search when the Search Audits page is first configured. The value of `false` indicates that MFT does not perform an audit search when the Search Audits page is first configured. Searches will be on demand when the user defines the selection criteria and click **Search**.

Parameter	Default	Description
SendGlobalEmail	`true`	This parameter is not used.
SendMFTTrustedCerts	`false`	True: When an FTPS client connects to the MFT FTPS Server, MFT returns a list of certificates that are defined to MFT as "Trusted Certificates". False: MFT does not send any trusted certificates to the FTPS Client.
SoapSkipFieldsConfigFileName	No default	When a customer uses SOAP calls and wants to upgrade MFT to a different version, setting this parameter will tell the SOAP calls to be compatible with older versions of MFT. Any RETRIEVE or GET call returns data in the format defined by MFT 7.2.4.
StatisticsUpdateInterval	`10`	MFT asynchronously updates the DB MFTStatistics table to improve performance. This parameter defines the frequency of statistics updates.
SyncLdapAtLogon	`true`	Defines whether an LDAP user will be synced with the LDAP authenticator when HTTP users log on. The value of `True` indicates that LDAP users are synced when the user logs on. The value of `False` indicates that LDAP users are not synced with the LDAP authenticator when the user logs on. The sync is performed when the On Demand or scheduled sync occurs.
TraceDir	The directory defined during installation	Defines the directory where MFT trace files are located.
TransferJMSThreadPoolSize	`100`	Defines the number of threads that is used to execute JMS Internet Server or Platform Server transfer requests. This parameter limits the number of concurrent JMS initiated transfers to the defined value.

Parameter	Default	Description
ValidationQueryTimeout	1	Defines the number of seconds that MFT waits for a DB Pooling validation query. If the query does not return in the defined number of seconds, the connection is closed and a new connection is created.
WebAdminLogFile	The directory defined during installation	Defines the directory where MFT WebAdmin files are located.
crystal_image_uri	/cfcc/control?view=view/cfcc/crystalreportviewers11	Defines the URL for the MFT reporting application.
net.sf.jasperreports.web.file.repository.root	No default	Defines the JasperSoft report root.  Do not change this parameter unless instructed to do so by MFT Technical Support.
reuseJMSConnection	false	True: Reuses JMS connections. False: Creates a new JMS connection for each request.  This parameter should be used for EMS only.
tilesDefinitions	/WEB-INF/tiles.xml	This parameter should not be changed.

Connectivity/Protocol Parameters

Connectivity and protocol parameters are associated with file transfers and file transfer protocols.

The following table lists the connectivity and protocol parameters:

Parameter	Default	Description
admincc-service-enabled	True	Enables the Command Center Admin API REST calls.
admin-service-enabled	True	Enables the Admin API REST calls.
ft-service-enabled	True	When Internet Server supports Admin (if admin server is enabled), it enables the file transfer API REST calls.

Parameter	Default	Description
AS2Acknowledgement	No default	When very large AS2 requests are to be received or sent, set this parameter to `deferred`. Encrypted AS2 data is written to the directory defined by the **AS2TempDirectory** parameter, and then processed.
AS2TempDirectory	No default	Defines the AS2 temporary directory generally only when very large (500MB+) AS2 files are transferred. This parameter tells MFT to use a two stage AS2 transfers. For Uploads to MFT, encrypted AS2 data is written to this directory before being transferred to the target internal MFT servers. For Downloads from MFT, encrypted AS2 data is written to this directory before being transferred to the target AS2 server. When this parameter is not defined, data is streamed from AS2 to the target server without writing to disk.
DisplayFTPBanner	`YES`	Defines whether the FTP/SFTP banner is displayed when the user logs on. `YES`: Indicates that the FTP/SFTP banner is displayed when the user logs on. `NO`: Indicates that the FTP/SFTP banner is not displayed when the user logs on.
FTPFileNameEncoding	`ISO-8859-1`	Defined the file name encoding for FTP connections. The default value of `ISO-8859-1` can work for most western European languages. For double byte languages, set this value to `UTF-8`.
FTPNumberOfPorts	None	Allows you to override the number of FTP ports used by this Internet Server instance. If defined, this parameter overrides the Systems Configuration: Global FTP Settings **Number of Ports to Use** parameter value.  This parameter is ignored for Command Center.
FTPStartingPort	None	Allows you to override the FTP starting port number used by this Internet Server instance. If defined, this parameter overrides the Systems Configuration: Global FTP Settings **Starting Port** parameter value.  This parameter is ignored for Command Center.

Parameter	Default	Description
MaxConnectionCnt	800 connections	Defines how many TCP connections are processed by each MFT protocol. This parameter applies to incoming FTP/FTPS, SSH and Platform Server connection requests. This parameter does not apply to HTTP or HTTPS. To configure the max HTTP/HTTPS connections , you must update the **maxConnections** parameter in the HTTP/HTTPS connector defined in the `server.xml` file.
SSHCipherSuite	All SSH ciphers	Defines the SSH cipher suites supported. When the MFT SFTP (SSH) server is started, it displays the SSH ciphers supported in the `catalina.out` file. Look for the header, SSH Server - supported ciphers.
SSHDigestSuite	All SSH Digest Suites	Defines the SSH digest suites supported. When the MFT SFTP (SSH) server is started, it displays the SSH ciphers supported in the `catalina.out` file. Look for the header, SSH Server - supported hash.
SSHFileNameEncoding	`ISO-8859-1`	Defined the file name encoding for SFTP (SSH) Connections. The default value of `ISO-8859-1` can work for most western European languages. For double byte languages, set this value to `UTF-8`.
SSHKeyExchange	All SSH Key Exchange algorithms except the unsecure "diffie-hellman-group1-sha1"	Defines the SSH key exchange algorithms supported. Some older SFTP clients might require "diffie-hellman-group1-sha1". When the MFT SFTP (SSH) server is started, it displays the SSH key exchange algorithms supported in the `catalina.out` file. Look for the header, SSH Server - supported key exchange.
SSHSecurityProvider	The default MFT security provider	Defines the security provider used by SFTP connections.
SSHServerHandshakeName	Internet Server SSHD	Allows the customer to update the response sent by the MFT Server when a connection is made to the MFT SSH Server.

Parameter	Default	Description
TCPBufSize	1024000	Defines the TCP buffer size used by SSH, FTP and Platform Server connections. Using a high value will increase performance over connections with high latency.
TLSCipherSuite	No default	Defines the cipher suites used by FTPS and Platform Server SSL connections. This parameter is used to limit the cipher suites used in creating FTP or Platform Server SSL connections. MFT will typically default to using secure cipher suites during installation.  HTTPS cipher suites are defined in the HTTPS connector in the *<MFT_Install>*/server/conf/server.xml directory.
TLSProtocols	TLSv1.2	Defines the protocols supported by FTP and Platform Server SSL connections. Valid values are:TLSv1.2, TLSv1.1, TLSv1
TLSSecurityProvider	The default MFT security provider	Defines the security provider used by FTP and Platform Server SSL connections.
TempDir	No default	Defines the temp directory that MFT uses when the virus scan is enabled.
UserSessionLimit	None	Defines the number of concurrent sessions that a user can have. By default, a user can have unlimited sessions. Be careful about setting this parameter too low. Some FTP or SFTP clients create a session for each concurrent transfer. So a transfer can fail if this parameter is set too low. Additionally, when a single user is utilized to perform automated transfers, these transfers can fail if this parameter is set too low.

RADIUS Authentication Parameters

RADIUS authentication parameters are used to configure RADIUS authentication.

The following table lists the RADIUS authentication parameters:

Parameter	Default	Description
RADIUS-Enabled	False	Defines whether all user ID and password authentication use the Radius protocol. The value of true indicates that all user ID and password authentication use the RADIUS protocol. The value of false indicates that the RADIUS protocol is not used.
The following parameter are available only when the **RADIUS-Enabled** parameter is set to True:		
RADIUS-BackupAdapterIP	No default	Defines the binding adapter IP address of the backup RADIUS host.
RADIUS-BackupHost	No default	Defines the IP address or name of the backup RADIUS host.
RADIUS-BackupPort	No default	Defines the port of the backup RADIUS host.
RADIUS-BackupSecret	No default	Defines the backup RADIUS server secret.  This parameter can only be set by using the **dbsettings** utility; it cannot be set manually. You must set this parameter using the **dbsettings** utility before performing the RADIUS authentication.
RADIUS-PrimaryAdapterIP	No default	Defines the binding adapter IP address of the primary RADIUS host.
RADIUS-PrimaryHost	No default	Defines the IP address or name of the primary RADIUS host.
RADIUS-PrimaryPort	No default	Defines the port of the primary RADIUS host.

Parameter	Default	Description
RADIUS-PrimarySecret	No default	Defines the primary RADIUS server secret.  This parameter can only be set by using the **dbsettings** utility; it cannot be set manually. You must set this parameter using the **dbsettings** utility before performing the RADIUS authentication.
RADIUS-SpecialUsers	No default	Defines users that will not be authentication by the RADIUS protocol. It is good practice to add one user (administrator) that is not authenticated by RADIUS.
RADIUS-Synchronous	`True`	Defines whether communication to primary and backup RADIUS servers is synchronous or asynchronous. The value of `True` indicates that the RADIUS authentication is synchronous. Communication to the backup RADIUS host will only be performed if communication to the primary RADIUS host times out. The value of `False` indicates that the RADIUS authentication is asynchronous. Requests will be made to both the primary RADIUS and backup RADIUS hosts at the same time. MFT will use the first response that is received.  This parameter is ignored if no backup RADIUS server is defined.
RADIUS-Timeout	`10`	Defines the RADIUS authentication timeout in seconds. If a response is not received in this amount of time, the request will fail.

OEM Parameters

OEM parameters are used to change the product names and branding.

The following table lists the OEM parameters:

Parameter	Default	Description
OEM-CommandCenterName	`Command Center`	Defines the text that is displayed when the product name of TIBCO MFT Command Center is displayed.
OEM-CompanyName	`TIBCO Software Inc.`	Defines the text that is displayed when the long company name is displayed on a web page.
OEM-CompanyURL	`http://www.tibco.com`	Defines the URL of the link to the TIBCO web site.
OEM-Copyright	`Copyright (c) 2003-2016. TIBCO Software Inc. All Rights Reserved.`	Defines the copyright information. This should not be changed. Changing this might be a violation of the TIBCO License Agreement.
OEM-InternetName	`Internet`	Defines the text that is displayed when the short product name of TIBCO MFT Internet Server is displayed.
OEM-InternetServerName	`Internet Server`	Defines the text that is displayed when the product name of TIBCO MFT Internet Server is displayed.
OEM-LongProductName	`TIBCO Managed File Transfer`	Defines the text that is displayed when the long product name is displayed on a web page.
OEM-PlatformName	`Platform`	Defines the text that is displayed when the short product name of TIBCO MFT Platform Server is displayed.
OEM-PlatformServerName	`Platform Server`	Defines the text that is displayed when the product name of TIBCO MFT Platform Server is displayed.
OEM-ProductURL	`http://www.tibco.com/products/automation/application-integration/managed-file-transfer/default.jsp`	Defines the URL of the link to the TIBCO web site for the MFT server.
OEM-ShortCompanyName	`TIBCO`	Defines the text that is displayed when the short company name is displayed on a web page.

Parameter	Default	Description
OEM-ShortProductName	MFT	Defines the text that is displayed when the short product name is displayed on a web page.

Database Driver Parameters

DB driver parameters are associated with the JDBC connection.

The following table lists the DB driver parameters:

Parameter	Default	Description
DBConn	The JDBC URL defined during installation	Defines the JDBC URL. This parameter rarely changes after MFT installation. It occasionally changes when you want to add SSL support or High Availability support.
DBDriver	The JDBC driver class name defined during installation	Defines the JDBC driver class. This parameter rarely changes unless you decide to change the JDBC driver used by MFT.
DBPass	The encrypted database password defined during installation	Defines the password of the database user associated with the JDBC connection.
DBPwdEncrypted	true	Defines whether the database password is encrypted.
DBUser	The database user defined during installation	Defines the database user associated with the JDBC connection.
OracleDatabaseSSLCipherSuites	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA SSL_DH_anon_WITH_RC4_128_MD5 SSL_RSA_WITH_3DES_EDE_CBC_SHA	Defines the cipher suites used by Oracle JDBC connections. Different Oracle server releases require different SSL cipher suites.

Database Pooling Parameters

DB pooling parameters are used to configure database pooling.

The following table lists the DB pooling parameters:

Parameter	Default	Description
DataBasePoolingFlag	APACHE	Defines whether connection pooling is supported. APACHE: Indicates that connection pooling is used. None: Indicates that connection pooling is not used.
MaxActive	400	Defines the maximum number of active connections available to database pooling. 400 active connections should be sufficient for all but the most active MFT system.
MaxIdle	20	Defines the maximum number of idle connections that must be kept in the database pool at all times.
MaxWaitTime	1	Defines the time in minutes that database pooling waits for a connection before the connection request fails.
MinEvictableIdleTime	4	Defines the time in minutes that a connection must be idle before it is eligible for eviction.
MinIdle	10	Defines the minimum number of idle connections that must be kept in the database pool at all times.
TestOnBorrow	true	Defines whether existing connections in the pool must be tested before use. It is good practice to set this parameter to true.
TestOnReturn	false	Defies whether existing connections in the pool must be tested after being used and returned to the pool. It is good practice to set this parameter to false.
TestWhileIdle	true	Defines whether connections should be tested while they are idle. Connections are tested based on the interval defined by the **TimeBetweenEvictionRuns** parameter.

Parameter	Default	Description
TimeBetweenEvictionRuns	2	Defines the time in minutes to sleep between execution of the idle connection validation classes.
ValidationQuery	SELECT COUNT(1) FROM FtpSrvCfg	Defines the query executed when the **TestOnBorrow**, **TestOnReturn** or **TestWhileIdle** parameter is set to true.
ValidatonQueryTimeout	1	The timeout in seconds before a connection validation query fails.
removeAbandoned	true	Defines whether to remove abandoned connections if they exceed the **removeAbandonedTimout**. If set to true, a connection is considered abandoned and eligible for removal if it has been idle longer than the **removeAbandonedTimeout**.
removeAbandonedTimeout	60	Defines the timeout in seconds before an abandoned connection can be removed..
logAbandoned	false	Defines whether to log stack traces for an application code which abandoned a statement or connection. (This parameter is used for debugging purposes only) In order to see logging of abandoned connections you must set logAbandoned to true in the web.xml and add the following line at the end of the logging.properties file in the server/conf directory. org.apache. tomcat.jdbc.pool.level = ALL It should show up in the console or in the catalina.log file

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for TIBCO® Managed File Transfer Internet Server is available on the TIBCO® Managed File Transfer Internet Server Product Documentation page.

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

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

Legal and Third-Party Notices