TIBCO® Managed File Transfer Internet Server

User Guide

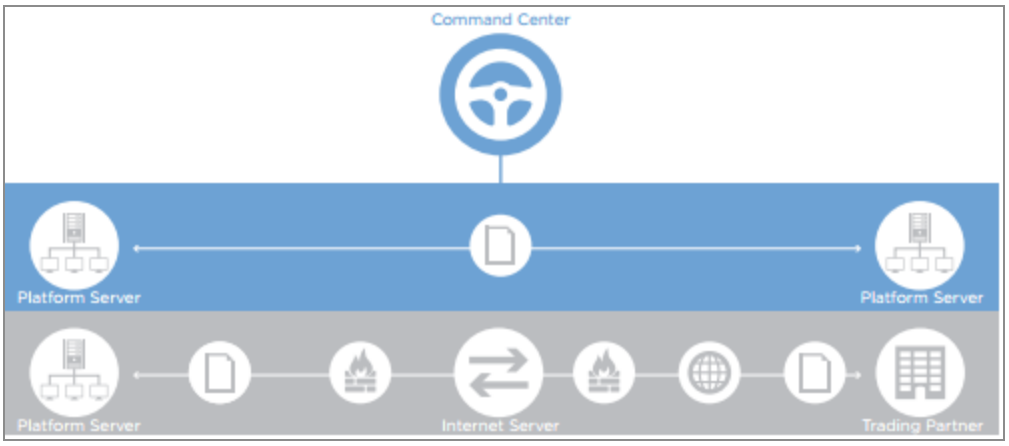
Version 8.5.0
March 2023

Contents

Product Overview

TIBCO® Managed File Transfer Internet Server provides a single point of control to manage all of your enterprise file transfers, both inside and outside the enterprise and across all major platforms (from Windows to the mainframe). It serves as the digital dashboard into your entire network; using a standard web browser, administrators can review and control all file-transfer activities, whether they are internal or external.

The following figure shows the system:



TIBCO MFT Internet Server provides the following benefits:

- **Security**

  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, GrammLeach-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.

- **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**

  Internet Server supports multiple protocols, including HTTP, HTTPS, FTP, FTPS (SSL), SFTP (SSH), AS2, CFI Protocol and many others.

- **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 backend system and never stored in the DMZ.

- **Easy to Use**

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

- **High availability and clustering**

  Support for clustering for failover and reliability.

Administrator Browser Configuration

You can configure TIBCO MFT Internet Server for use through the Administrator web pages, the command-line interface, and REST calls.

Accessing the Administrator Browser

After installing and configuring TIBCO MFT Internet Server, you can access the Administrator web pages.

Procedure

1. Use the following URL to log in by substituting the parts of the URL with your installation configurations:

   `https://[HostName]:[Port]/cfcc/control?view=view/admin/start.jsp`

   Where hostname is the IP name of the Command Center and the default port is 7443.

   Optionally, if you have configured the root shortcuts, you can access the pages with this URL:

   `https://HostName:Port/admin`

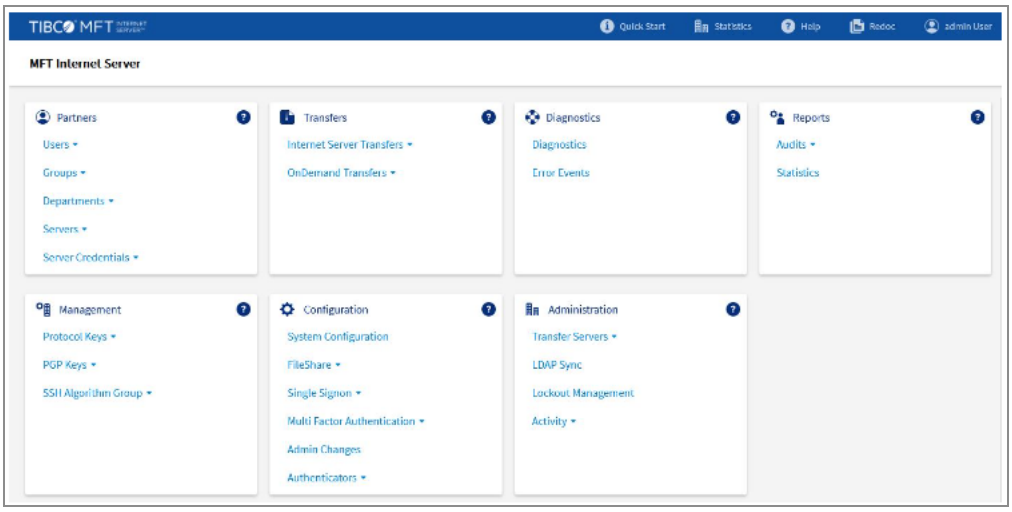
2. Enter the administrator default username and password.

   The default user id is `admin`. The default password is `changeit`.

   We strongly suggest changing the admin password immediately.

3. Click **Sign In** and the TIBCO MFT Internet Server admin home page is displayed.

Admin Home Page Overview



To return to the landing page from any page, click the product name in the upper left corner of the page:

TIBCO MFT Internet Server

Icon/Tab	Description
The product logo	Displayed on all pages. If you click this logo from any page, you can access the admin home page.
Quick Start	Displayed on the upper-right side of the page. If you click this logo from any page, you can access the Quick Start Guide.
Statistics	Displayed on the upper-right side of the page. This tab is displayed only on the home page. Click **Statistics** to display the summary of transfer statistics.
Help	Displayed on the upper-right side of the page. This icon displays detailed help information about the page you are accessing and all parameters on the page. This is displayed on all admin pages. **Note:** This guide provides general information about the admin pages. Detailed information is provided on the help pages.

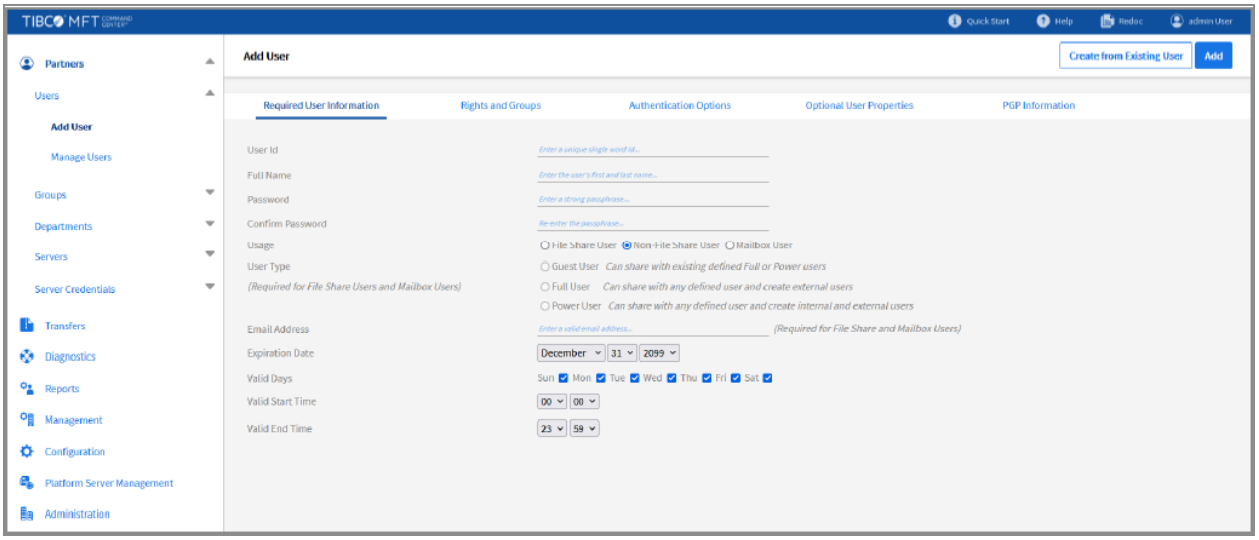
Icon/Tab	Description
Redoc	Displayed on the upper-right side of the page. This tab displays the pane containing the links to view the API documentations for REST calls.
Administrator account	Displayed on the upper-right side of the page. Click on the **Administrator account** tab to change your password or to sign out.

On the landing page, you can click on any line in any of the boxes. An arrow down next to the line indicates that this line is a heading and can be expanded. An arrow up indicates that the line has been expanded and can be contracted. If a line has no arrow up or down, this is a link. Note that some lines can be expanded multiple times before a link is displayed that allows you to access a particular admin page.

For example, if you click **Users**, two links are displayed:

- **Add User**
- **Manage User**

If you click **Add User**, the **Add User** page is displayed. See below.



The left side of each admin page, other than the landing page, has navigation links that you can use to execute any page without returning to the landing page. You can expand and contract the line by clicking on the line. Just like the landing page, an arrow down indicates that the line can be expanded, an arrow up means that the line has been expanded and can be contracted and no arrow indicates that this is a link.

To return to the landing page from any page, click the product name in the upper left corner of the page:

When you click any link on the home page, you are redirected to a new page to perform that task. You can go to other pages by clicking the links on the left-side navigation page. For example, when you navigate to the **Users > Add User** page, you can go to other pages by clicking the link in the left-side navigation.

Partners

As an administrator, you can define access points into the system. Specifically, the **Partners** page allows you to configure users, groups, departments, servers, and server credentials.

Users

As an administrator, you can define the attributes, rights, and credentials for users that access MFT. The user pages allow you to create, manage, delete, and update users. User definitions are required for:

- Every user that accesses the admin pages.
- Every user that accesses MFT Internet Server through a transfer client (Browser, FTP, SFTP, Platform Server, AS2)

Rights

The rights required to view and update users are:

Right	Description
AdministratorRight	Allows you to view or update all users.
UpdateTransferUserRight	Allows you to view, add, and update users. You can update users that only have `TransferRight`, but you cannot update admin users.

Right	Description
UpdateExistingTransferUserRight	Allows you to update users. You can update users that only have `TransferRight`, but you cannot update admin users.
ViewUserRight	Allows you to view users, but you cannot update users.
ViewGroupRight UpdateGroupRight	One of these rights is required to view or update users.
HelpDeskRight	Allows you to view users and allows you to update limited user properties: • Password • Disabled/locked flag • Password reset flags

Tasks

There are two links displayed for users:

Task	Description
Add Users	Allows you to create a new user definition.
Manage Users	Allows you to list and manage all users. You can define **Search Criteria** to display only users that match the criteria. Once a list of users is displayed, you can click **User Id** and the **Update User** page is displayed. You can also delete users from the **Manage Users** page.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage

this department.

Adding Users

As an administrator, you can add a new user. The user information can be entered on this page. To add a new user, complete the following steps.

Procedure

1. Click **Add User**.
2. Enter the required information described in the table below:

Tab	Description
Required User Information	Defines mandatory parameters that you must configure.
Rights and Groups	Defines assigned rights and group membership. Each user must be granted administrative and transfer rights to perform admin functions or transfer files. On the "Add User" page, `TransferRight` is selected by default. If you do not want to assign `TransferRight` for a user, you must remove this right. Groups are a way to give multiple users rights to perform transfers. The **Internet Server Transfers** page includes information about how to assign users or groups to a transfer definition.
Authentication Options	Defines how you want this user to authenticate to perform transfers for the client transfer protocols supported by the TIBCO MFT Server. You can define authentication methods for FTP, SFTP, HTTPS, and Platform Server.
Optional User Properties	Defines more advanced user properties, including: • Department parameters for delegated administration • Transfer date/time restrictions • Password parameters • Restricting users based on their IP address

Tab	Description
PGP Information	Defines whether this user is allowed to add PGP public keys.

Note: To automatically select values from an existing user, click **Add From Existing User** and select the user link.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.
4. After clicking **Add User**, an info message pops up that allows you to create PGP or Protocol Keys for this user. After clicking on the link, the following tabs are displayed.

Tab	Description
PGP Public Keys	Defines parameters which are required to enter to add a PGP Public Key.
Protocol Public Keys	Defines parameters which are required to enter to add a Protocol Public Key.

Note:

- To go back to the Add User page, click the **Back to Add User** button.
- The logged-in user must have either PGP or Protocol keys rights to add the PGP or Protocol Key.

Managing Users

The **Manage Users** page displays the first 100 user records defined in the TIBCO MFT server. It also gives you the capability to search the user record database to limit the number of user records displayed. There are two options to manage users:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the user record database to limit the number of records that are displayed on the user results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 user records are displayed within the **Results** table. If you click the User ID of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating User Information

To update an existing user information, complete the following steps.

Procedure

1. Click the user ID from the **Results Table**.

   The **Update User** page is displayed.
2. Enter the required changes.
3. Click **Update**.

To return to the users list, click **Back to Users List**.

Deleting a User

When deleting a user definition, the System Configuration **Check Dependency Before Delete** parameter determines if a dependency check is performed. When enabled, prior to deleting a user definition, a dependency check is performed for the following:

- Internet Transfer definitions
- PGP Public Keys

- Protocol Public Keys
- Scheduler Jobs with Job Type "Internet Transfer"

If a dependency exists, a warning message is displayed. Based on the **Check Dependency Before Delete** setting, you are given the option to delete the user definition.

To delete a user, complete the following steps:

Procedure

1. Select the checkbox next to the user that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

Groups

As an administrator, you can define file transfer groups. Users can be members of multiple file transfer groups. File transfer groups can be assigned to transfer definitions to enable all users in the group to perform file transfers. The group pages allow you to create, manage, delete, and update groups.

You can also assign users to groups in these pages or you can use the **Add/Update User** pages to assign users to groups.

Rights

The rights required to view and update groups are:

Right	Description
AdministratorRight	Allows you to view or update all groups.
ViewGroupRight	Allows you to view groups but you cannot update groups.
UpdateGroupRight	Allows you to view or update all groups

Tasks

There are two links displayed for users:

Task	Description
Add Group	Allows you to create a new group definition
Manage Groups	Allows you to list and manage all groups. Once a list of groups is displayed, you can click **Group Id** and the **Update Group** page is displayed. You can also delete groups from the **Manage Groups** page.

Delegated Administration

Administration can be delegated to groups in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage this department.

Adding Groups

As an administrator, you can add a new group. The group information can be entered on this page. To add a new group, complete the following steps.

Procedure

1. Click **Add Group**.
2. Enter the required information described in the table below:

Tab	Description
Required Group Information	Defines mandatory parameters that you must configure.
Assign Users to Group	Allows you to assign users to groups.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Note: To automatically select values from an existing group, you can click **Add From Existing Grou**p and select the Group link.

Managing Groups

The **Manage Groups** page displays the groups defined in the TIBCO MFT server. You can manage groups using the **Results Table**.

Results Table

Group records are displayed within the **Results** table. If you click the Group ID of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized.

Updating Group Information

To update an existing group information, complete the following steps.

Procedure

1. Click the existing Group ID from the **Results Table**.

   The **Update Group** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Group

To delete a group, complete the following steps.

Procedure

1. Select the checkbox next to the group that you want to delete.
2. Click the delete icon.

3. When prompted, click **OK**.

Departments

As an administrator, you can define departments. Users can be members of one department but can be configured to manage multiple departments. The department pages allow you to create, manage, delete, and update departments. You cannot assign users to departments in these pages. You must use the **Add/Update User** pages to assign users to a department.

Rights

The rights required to view and update departments are:

Right	Description
AdministratorRight	Allows you to view or update all departments.

Tasks

There are two links displayed for users:

Task	Description
Add Department	Allows you to create a new department.
Manage Departments	Allows you to list and manage all departments. Once a list of departments is displayed, you can click **Department Name** and the **Update Department** page is displayed. You can also delete departments from the **Manage Departments** page.

Delegated Administration

Delegated Administration uses departments. Only super administrators can add or update departments.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Delegated administration allows you to delegate administration of transfer, users, and servers to particular users. Users can then only administer transfer, users, and servers assigned to their department or departments they can manage.

Adding Departments

As an administrator, you can add a new department. The department information can be entered on this page. To add a new department, complete the following steps.

Procedure

1. Click **Add Department**.
2. Enter the required information in the **Required Department Information** tab. This defines mandatory parameters that you must configure.
3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing Departments

The **Manage Departments** page displays the departments defined in the TIBCO MFT server. You can manage departments using the **Results Table**.

Results Table

Department records are displayed within the **Results** table. If you click the department name of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized.

Updating Department Information

To update an existing department information, complete the following steps.

Procedure

1. Click the existing department name from the **Results Table**.

   The **Update Department** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Department

To delete a department, complete the following steps.

Procedure

1. Select the checkbox next to the department that you want to delete.
2. Click the **Delete** icon.
3. When prompted, click **OK**.

Servers

As an administrator, you can define file transfer servers. A server defines the connectivity information required to connect to a target server to transfer files with that server. Transfer definitions define both the user authorized to perform the transfer as well as the server where the files will reside. The Server pages allow you to create, manage, delete, and update servers.

Server definitions also define management parameters. You can configure transfer servers to perform Platform Server Management, DNI Management, and Server Status Management.

Rights

The rights required to view and update servers are:

Right	Description
AdministratorRight	Allows you to view or update all servers.

Right	Description
ViewServerRight	Allows you to view servers but you cannot update servers.
UpdateServerRight	Allows you to view or update all servers.

Tasks

There are two links displayed for servers:

Task	Description
Add Server	Allows you to create a new server definition.
Manage Servers	Allows you to list and manage all servers. Once a list of servers is displayed, you can click **Server Name** and the **Update Server** page is displayed. You can also delete servers from the **Manage Servers** page.

Delegated Administration

Administration can be delegated to servers assigned to a department in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage this department.

Adding Servers

As an administrator, you can add a new server. The server information can be entered on this page. To add a new server, complete the following steps.

Procedure

1. Click **Add Server**.
2. Enter the required information described in the table below:

Tab	Description
Required Server Information	Defines mandatory parameters that you must configure. This includes connectivity information, server type, and server platform.
Server Options	Defines a server file name prefix. If defined, this parameter is prefixed to the server file name for all transfers with this server. This tab is not displayed for all Server types.
Server Credentials	Defines the credentials needed to access this server.
Proxy Properties	Defines the proxy server parameters for this server. Proxy properties are supported for the following protocols: SSH, HTTP, Amazon S3, Microsoft Azure, Sharepoint, Google Storage. **Note:** Proxy properties support all operations except download for the Sharepoint and ADLS Gen2 Storage protocol. See help pages for more information about Proxy Properties.
Additional Server Properties	Defines miscellaneous server properties, including the department of this server. The other parameters are rarely used.
Management Options	Defines the following functions: • pDNI Daemon management properties • Command Center Collection properties for Platform Transfers • Server status properties for all servers
PGP Information	Defines PGP parameters used when PGP encrypting and signing files sent to the target server, or PGP decrypting and verifying files received from the target server. See *MFT Internet Server Quick Start Guide* for more information on configuring PGP for users, transfers, and servers.

Tab	Description
Anti Virus Properties	Defines antivirus configuration properties. These properties allow you to enable antivirus checking for transfers to this node. You can also define the antivirus mode (Streaming or Store and Forward as well) and the REGEX that defines whether files are scanned for violations.
DLP Properties	Defines DLP configuration properties. These properties allow you to enable DLP scanning for transfers to this server. You can also define the DLP mode (Streaming or Store and Forward) and REGEX that defines whether files are scanned for violations.

The following tabs are displayed only when the **Server Type** is set to certain values. For example, the **SSH Options** tab is only displayed when the **Server Type** is set to SSH.

Task	Description
Platform Server Options	Defines security information such as encryption used and private keys used by Platform Server SSL and tunnel connections. This tab is displayed only when the server type is `Platform Server`. The parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `Platform Server`. MFT Internet Server initiates a connection to the target Platform Server using these parameters.
Microsoft Azure Options	Defines Microsoft Azure information including storage type and performance parameters like chunk sizes, buffer, authentication type, and thread counts. This tab is displayed only when the server type is `Microsoft Azure`. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `Microsoft Azure`. MFT Internet Server initiates a connection to the target Microsoft Azure server using these parameters.

Task	Description
Google Cloud Options	Defines Google Cloud information including storage type and performance parameters like chunk sizes and buffers. The service account credentials are also stored in this tab. The credentials tab is ignored for transfers to Google Cloud servers. This tab is displayed only when the server type is `Google Cloud`. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `Google Cloud`. MFT Internet Server initiates a connection to the target Google Cloud server using these parameters.
Custom Server Options	Defines custom servers that provide an API that allows you to add support for protocols not supported by MFT Internet Server. This tab is displayed only when the server type is `Custom Server`. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `Custom Server`.
Internet Server Options	Defines the MFT Internet Server context for the connection using HTTPS. This is used only when the Command Center initiates an Internet Server Transfer and connects to Internet Server to initiate the Internet Server transfer.
FTP Options	Defines FTP information such as the data connection type, security information used for SSL or TLS connections, and whether connections to the target server are pooled. It also defines an FTP private key that can be used for certificate authentication to the target server. This tab is displayed only when the Server Type is **FTP**. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `FTP`. MFT Internet Server will initiate a connection to the target FTP Server using these parameters.
SSH Options	Defines SSH information including whether connections to the target server are pooled. It also defines an SSH private key that can be used for key or certificate authentication to the target server. This tab is

Task	Description
	displayed only when the Server Type is SSH. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as SSH. MFT Internet Server will initiate a connection to the target SSH server using these parameters.
HDFS Options	Defines HDFS security information. This tab is displayed only when the server type is HDFS, that is, Hadoop. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as HDFS. MFT Internet Server will initiate a connection to the target HDFS server using these parameters.
HTTP Options	Defines the system key that you can use when performing certificate authentication to a target HTTPS server. This tab is displayed only when the server type is HTTP. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as HTTP.
AS2 Options	Defines many parameters used for AS2 transfers, including local and partner AS2 IDs, system keys, public keys, and incoming and outgoing AS2 parameters. This tab is displayed only when the server type is AS2. AS2 servers are used in the following ways: • When a transfer client initiates a transfer and the transfer definition points to a server definition configured as AS2. When an AS2 transfer client initiates a transfer to Internet Server. MFT Internet Server matches the incoming Partner ID with the Partner ID defined in the server definition. AS2 transfers are complicated to configure. For more information about configuring incoming and outgoing AS2 transfers see *MFT Internet Server Quick Start Guide* on.
Amazon S3 Options	Defines Amazon S3 information including performance parameters, such as chunk sizes, buffer, and thread counts. There is also

Task	Description
	information specific to Amazon S3 and some security parameters. This tab is displayed only when the server type is `Amazon S3`. Parameters in this tab are used when a transfer client initiates a transfer and the transfer definition points to a server definition configured as `Amazon S3`. MFT Internet Server initiates a connection to the target Amazon S3 server using these parameters.
Email Options	Defines options that can be set when files are sent as email attachments. You can define options including TLS options, default sender email address, maximum attachment size, and whether transfers are allowed only to predefined users.
Mailbox Options	Defines options that can be set when files are sent as mailbox attachments. You can define options including default sender email address, maximum attachment size, default expiration, and whether transfers are allowed only to predefined users.
SharePoint Options	Defines options that can be configured when the **Server Type** is set to `Sharepoint`. You can define the number of upload buffers and the upload chunk size.
JMS Server Options	Defines information that overrides the Global JMS service. Parameters in this tab such as JMS Context Factory, Queue, Connection Factory, and Topic Connection Factory override the Global JMS Service.
OFTP2 Options	Defines options that can be configured when the **Server Type** is set to `OFTP2`. You must define the information required for incoming and outgoing OFTP2 connections. This information includes Local and Remote Odette IDs and passwords.

The **Add Server** and **Manage Servers** pages allow you to configure a variety of information. The tabs displayed depend on the Server Type defined. Not all tabs are displayed. For example, if you configure the Server Type as "Platform Server", the following tabs are not displayed: FTP Options, SSH Options, HDFS Options, HTTP Options, AS2 Options, Amazon S3 Options, Microsoft Azure Options, Google Cloud

Options, Customer Server Options, SharePoint Options, OFTP2 Options, and Internet Server Options.

Note:

- To automatically select values from an existing server, you can click Add From Existing Server and select the server link from the Add from Existing Server page.
- Passwords are not copied from the source server to the target server.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.
4. After clicking **Add Server**, an info message pops up that allows you to create PGP or Protocol Keys for this user. After clicking on the link, the following tabs are displayed.

Tab	Description
PGP Public Keys	Defines parameters which are required to enter to add a PGP Public Key.
Protocol Public Keys	Defines parameters which are required to enter to add a Protocol Public Key.

Note:

- PGP must be enabled in the PGP information tab to add a PGP key for a server.
- To go back to the Add Server page, click the **Back to Add Server** button.
- The logged-in user must have either PGP or Protocol keys rights to add the PGP or Protocol Key.
- When adding a Server that requires you to retrieve a Server key or certificate, an info message pops up that allows you to navigate to the **Update Server** page to retrieve the key or certificate for that server.

Managing Servers

The **Manage Servers** page displays the first 100 server records defined in the TIBCO MFT server. It also gives you the capability to search the database to limit the number of server records displayed. There are two options to manage servers:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively limit the database to limit the number of records that are displayed on the server credentials results table. The percent sign (%) is used as a wild-card character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 server records are displayed within the **Results** table. If you click the server name of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Server Information

To update an existing server, complete the following steps.

Procedure

1. Click the **Server Name** type from the **Results Table**.

   The **Update Server** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Server

When deleting a Server definition, the System Configuration **Check Dependency Before Delete** parameter determines if a dependency check is performed. When enabled, prior to deleting a server definition, a dependency check is performed for the following:

- Scheduler jobs
- Internet Transfer definitions
- Platform Transfer definitions
- PGP Public Keys
- Protocol Public Keys

If a dependency exists, a warning message is displayed. Based on the **Check Dependency Before Delete** setting, you are given the option to delete the server definition.

To delete a server, complete the following steps.

Procedure

1. Select the checkbox next to the server that you want to delete.
2. Click the **Delete** icon.
3. When prompted, click **OK**.

Server Credentials

As an administrator, you can define server credentials. Server credentials define a way to granularly define credentials when accessing target servers. By default, the server definition defines the credentials used when connecting to target servers. Server credentials allow you to define credentials for defined users connecting to defined servers. The Server Credential pages allow you to create, manage, delete, and update server credentials.

Rights

The rights required to view and update server credentials are:

Right	Description
AdministratorRight	Allows you to view or update all server credentials.
ViewServerCredentialRight	Allows you to view server credentials but you cannot update server credentials.
UpdateServerCredentialRight	Allows you to view or update all server credentials.

Tasks

There are two links displayed for server credentials:

Task	Description
Add Server Credentials	Allows you to create a new server credentials.
Manage Servers Credentials	Allows you to list and manage all server credentials. Once a list of server credentials page is displayed, you can click **ID Type** and the **Update Server Credentials** page is displayed. You can also delete server credentials from the **Manage Server Credentials** page.

Delegated Administration

Server credentials are not assigned to a department. Server credentials are associated with the server definition department. Administration can be delegated to server credentials by updating in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to the server department or can manage the server department can assign server credentials to this department.

Adding Server Credentials

As an administrator, you can add new server credential. The server credential information can be entered on this page. To add a new server credential, complete the following steps.

Procedure

1. Click **Add Server Credentials**.
2. Enter the required information described in the table below:

Tab	Description
Required Server Credential Information	Defines mandatory parameters that you must configure.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing Server Credentials

The **Manage Server Credentials** page displays the first 100 server credential records defined in the TIBCO MFT server. It also gives you the capability to search the database to limit the number of server records displayed. There are two options to manage servers:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the database to limit the number of records that are displayed on the server results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 server credential records are displayed within the **Results** table. If you click the **Id Type** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Server Credential Information

To update server credential information, complete the following steps.

Procedure

1. Click the **Id Type** from the **Results Table**.

   The **Update Server Credential** page is displayed.
2. Enter the required changes.
3. Click **Update**.

To return to the server list, click **Back to Search**.

Deleting a Server Credential

To delete a server credential, complete the following steps.

Procedure

1. Select the checkbox next to the server that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

Transfers

As an administrator, you can configure Internet and Platform transfers, and execute Platform transfers. You can also configure alerts for Internet and Platform transfers. OnDemand transfer properties can also be configured.

Internet Server Transfers

As an administrator, you can give access to a user to initiate a transfer to a target server. Transfer definitions define the following information:

- Users who are authorized to perform a transfer

- Target server file names
- The target server for file transfers
- Postprocessing actions
- Other miscellaneous transfer parameters

Since transfer definitions include the user who is authorized to perform a transfer and the transfer target server, you must create the user definition and the server definition before creating a transfer definition.

Rights

The rights required to view and update transfer definitions are:

Right	Description
AdministratorRight	Allows you to view or update all transfer definitions.
ViewTransferRight	Allows you to view transfer definitions but you cannot update transfer definitions.
UpdateTransferRight	Allows you to view or update transfer definitions.

Tasks

There are two tasks displayed for transfers:

Task	Description
Add Transfer	Allows you to create a new transfer definition.
Manage Transfers	Allows you to list all transfers. You can define **Search Criteria** to display only transfer definitions that match the criteria. Once a list of transfers is displayed, you can click **Transfer Id** and the **Update Transfer** page will be displayed. You can also delete transfers from the **Manage OnDemand Sites** page.

Delegated Administration

Administration can be delegated to a department that is assigned transfer definitions in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage this department.

Adding Transfers

The TIBCO MFT Server allows you to add a new transfer. The transfer information can be entered on this page. To add a new transfer, complete the following steps.

Procedure

1. Click **Add Transfer**.
2. Enter the required information described in the table below:

Tab	Description
Required Transfer Information	Defines parameters that you must configure. These include the file names, authorized users and groups, and the target server. You also must determine if the transfer is an upload, download, or both. When **Both** is selected, two transfer definitions are created; one for download and one for upload. The Virtual Alias must be defined. When an authorized user connects to the TIBCO MFT Server and issues a directory list, the virtual alias is returned. This allows TIBCO MFT Server to hide the actual locations of the target files from the transfer users.
Server Properties	Allows you to override credentials defined on the server definition. It also allows you to override the SSH private key used when using SSH key authentication to a target SSH server.
Additional Transfer Properties	Defines many miscellaneous transfer properties, including: • Transfer description

Tab	Description
	• Data properties • Accessibility • Checkpoint properties • File transfer rules • Tracing
Email Notification	Defines parameters associated with sending emails. Emails can be sent two ways: • When a transfer definition is created to notify a user that files are ready to be uploaded or downloaded. • More commonly, emails can be sent to users when a transfer executes, either successfully or unsuccessfully.
Postprocessing Actions	Defines the postprocessing actions associated with the transfer definition. Up to four postprocessing actions can be executed, based on either transfer success or failure.
z/OS Properties	Defines z/OS properties that are used when creating files on a z/OS mainframe. The z/OS properties are only used when the server type is FTP or Platform Server.
UNIX Properties	Defines UNIX file permissions when files are created on a target Platform Server for UNIX. Otherwise, this box is ignored.
PGP Information	Defines PGP parameters, when a transfer client downloads a file, the file can be PGP encrypted and signed. When a transfer client uploads a file, the file can be PGP decrypted and the signature verified. For more information about configuring PGP for users, transfers, and servers, see the *MFT Internet Server Quick Start Guide*.
Antivirus properties	Displayed only when antivirus checking is enabled on the System Configuration. Allows you to enable or disable antivirus checking,

Tab	Description
	define the antivirus mode, and a REGEX to select files to check for viruses.
Client Permissions	Defines various file transfer permissions. For example, you can allow a client to rename or delete a file. A user can also restrict transfer by IP address or IP name by selecting the **Restrict Transfer** option.
JMS Properties	Defines JMS properties and selectors. This tab is only displayed when the server type is JMS.
Email Properties	Defines properties used when the server is defined as an Email server. This means that files are sent as attachments to an email.
Mailbox Properties	Defines properties used when the server is defined as a mailbox server. This means that files are sent as an Internet Server Mailbox request. Files are stored in a repository and an email is sent to the defined user telling them that a file is ready to be downloaded.
HTTP Properties	Defines parameters when the target server is defined as an HTTP server. Files can be uploaded or downloaded through an HTTP stream or an HTTP form.
SharePoint Properties	This tab is only displayed when the "Server Name" is a SharePoint server. This tab allows you to define a document library URL that is appended to the SharePoint URL defined in the server definition.
OFTP2 Properties	This tab is only displayed when the "Server Name" is an OFTP2 server. You can define parameters specific to a transfer, including OFTP2 record format, maximum record size and virtual file descriptions.
DLP Properties	Displayed only when DLP checking is enabled on **System Configuration**. Allows you to enable or disable DLP scanning, define the DLP mode, and a REGEX to select files to scan for violations.

> **Note:** To automatically select fields from an existing transfer, you can click on **Add From Existing Transfer** and select the transfer link.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing Transfers

The **Manage Transfers** page displays the first 100 transfer records defined in the Command Center server. It also gives you the capability to search the database to limit the number of transfer records displayed. There are two options to manage transfers:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the transfer definitions to limit the number of definitions that are displayed in the **Results** table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a transfer definition is returned. When you have completed the **Search Criteria**, click the **Search** button to perform the search and create the **Results** table.

Results Table

Up to 100 transfer definitions are displayed within the **Results** table. If you click the transfer ID of one of the entries in this table, the **Update Transfer** page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Transfer Information

To update an existing transfer information, complete the following steps.

Procedure

1. Click the existing **Transfer Id** from the **Results Table**.

   The **Update Transfer** page is displayed.
2. Enter the required changes.
3. Click **Update**.

To return to the transfers list, click **Back to Transfers List**.

Deleting a Transfer

When deleting a transfer definition, the System Configuration **Check Dependency Before Delete** parameter determines if a dependency check is performed. When enabled, prior to deleting a transfer definition, a dependency check is performed for the following:

- Scheduler Jobs of type **Internet Transfer** that are configured to this transfer definition.

If a dependency exists, a warning message is displayed. Based on the **Check Dependency Before Delete** setting, you are given the option to delete the transfer definition.

To delete a transfer, complete the following steps.

Procedure

1. Select the checkbox next to the transfer that you want to delete.
2. Click the **Delete** icon.
3. When prompted, click **OK.**

OnDemand Transfers

As an administrator, you can give access to a user to utilize the Desktop Client OnDemand transfer capability.

The OnDemand Transfer capability allows a desktop client user to perform transfers to target FTP, SSH, or Platform Server requests without making the configuration entries required by standard transfers. This page allows you to create rules to restrict or approve hosts that can be used by different users or departments. It also allows you to define the protocols that can be used.

Rights

The rights required to view and update transfer definitions are:

Right	Description
AdministratorRight	Allows you to view or update all OnDemand transfer definitions.
ViewOnDemandRight	Allows you to view on demand transfer definitions but you cannot update OnDemand transfer definitions.
UpdateOnDemandRight	Allows you to view or update OnDemand transfer definitions.

Tasks

There are two tasks displayed for transfers:

Task	Description
Add OnDemand Site	Allows you to create a new transfer definition.
Manage OnDemand Sites	Allows you to list all OnDemand sites. You can define **Search Criteria** to display only OnDemand sites that match the criteria. Once a list of transfers is displayed, you can click **Site Name** and the **Update OnDemand Transfer** page is displayed. You can also delete transfers from the **Manage Transfers** page.

Delegated Administration

Administration can be delegated to a department that is assigned OnDemand transfer definitions in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage this department.

Adding OnDemand Site

The TIBCO MFT Server allows you to add a rule that will allow users to utilize the OnDemand Transfer capability. The transfer information can be entered on this page. This page allows you to create rules to restrict or approve hosts that can be used by different users or departments. It also allows you to define the protocols that can be used. Rule checking will be performed based on the following order of precedence from high to low:

1. User ID has exact match
2. User ID has wild card match
3. User's department has exact match
4. User's department has wild card match
5. All users have an exact match
6. All users have a wildcard match
7. Request will be denied if no rule exists for the user

To add a new site, complete the following steps.

Procedure

1. Click **Add OnDemand Site**.
2. Enter the required information in the **Required OnDemand Site Information** tab. This defines mandatory parameters that you must configure. These include the site name, description, IP addresses, authorized users, and groups that can connect to the target server.
3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing OnDemand Sites

The **Manage OnDemand Sites** page displays the first 100 site names defined in the Command Center server. It also gives you the capability to search the database to limit the number of user records displayed. There are two options to manage OnDemand sites:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to limit the number of OnDemand Sites that are returned. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a transfer definition will be returned. When you have completed the **Search Criteria**, click the **Search** button to perform the search and create the **Results** table.

Results Table

Up to 100 sites are displayed within the **Results** table. If you click the site name of one of the entries in this table, the **Update Transfer** page is displayed that also allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating OnDemand Site Information

To update an OnDemand site information, complete the following steps.

Procedure

1. Click the existing **Site Name** from the **Results Table**.

   The **Update OnDemand** page is displayed.
2. Enter the required changes.
3. Click **Update**.

To return to the transfers list, click **Back to Site List**.

Deleting an OnDemand Site

To delete an OnDemand site, complete the following steps.

Procedure

1. Select the checkbox next to the site that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK.**

Diagnostics

Administrators can view diagnostics and debugging information for Internet Server and Command Center instances.

Diagnostics

As an administrator, you can display debugging information about the MFT hosts. As an administrator, you can display information about the Command Center or Internet server instance. When you first enter this page, diagnostic information is displayed for the server your browser is connected to. Select the server name of the diagnostics you want to see.

The **Diagnostics** page displays information for the selected Internet Server or Command Center instance. This information is often required by TIBCO Technical support when a case is opened. The following list indicates some of the information displayed:

- Version information
- JVM Settings
- Active Transfers
- Server Time Settings
- JVM System Properties
- Environment Variables
- Cipher Suites
- web.xml parameters
- Trace Settings
- File Information

When the **Diagnostics** page is first displayed, the diagnostic information for the Internet Server or Command Center instances that you are logged into is displayed. The "Select Server" drop-down box allows you to select a server to display diagnostics. You can also click the **Save Server Diagnostics to File** button to save the diagnostics to a file. Do this when opening a support case with TIBCO MFT Support.

To see the types of information that are displayed, see the following table.

Type of Information	Description
Diagnostics	Displays diagnostic information about the Internet Server and Command Center hosts in the MFT Cluster.
Events	Displays information about the events that have been executed in the MFT Cluster.
Error Events	Displays information about error events that have been executed in the MFT Cluster.
Server Status	Displays whether monitored servers are active or inactive.

Rights

The **AdministratorRight** is required to view diagnostics.

Tasks

Diagnostic Information defines a variety of diagnostic information. This information is often used by TIBCO Technical Support when debugging problems.

Delegated Administration

Users assigned to a department cannot view diagnostics information. Only the super administrator can view diagnostics.

Error Events

As an administrator, you can display information about error events that have occurred. Error events are typically created when a directory list request fails. It allows you to determine the cause of the failure directory list failure.

Rights

The rights required to view events are:

Right	Description
AdministratorRight	Allows you to view error events.
ViewAuditRight	Allows you to view error events.
HelpDeskRight	Allows you to view error events.

Delegated Administration

Administration can be delegated to department users that create error event records by users with the required rights that are not assigned to a department.

Searching Error Events

As an administrator, you can search for error events. The error event information can be entered on this page. To search for error events, complete the following steps.

Procedure

1. Click **Search Criteria**.
2. Enter the required information.

   Note: The **Search Criteria** allows you to filter the error events that are displayed. The **Results** table displays the results of your search.

3. When you have finished entering the information, click the **Search** button.

Viewing Error Event Detail Information

To view the detailed information for an error event, click the existing **Error Id** from the **Search Criteria Results** table. The **Error Event Details** page is displayed.

Reports

MFT allows the admin to display reports on transfers and alerts. The **Reports** pages also provide a variety of dashboards and reporting mechanisms. In these pages, you can

- Display summary and transfer dashboards
- Search for completed transfers display detailed information about transfers.
- Search for alerts and display detailed information about alerts.
- Display MFT transfer statistics.
- Create a variety of database reports.

Audits

As an administrator, you can display summary and detail information about completed Internet Server and Platform Server transfers. You can do perform these functions from within the **Audits** pages:

- Search Audits
- Delete Audits
- Resubmit Results
- Audit Search Filters

Searching Audits

As an administrator, you can search for completed Internet Server and Platform Server audit records. There are three components of the **Search Audits** page:

- Search Criteria
- Platform Server Manual Poll Criteria
- Results Table

Search Criteria

Search Criteria allows you to define filters to the transfers that are displayed. There are a variety of filter parameters, including transaction IDs, file names, User IDs, start date, start time, end date, and end time. You can define whether to search for Internet Server transfers, Platform Server transfers, or both. You can also select a predefined **Audit Search** filter on this page.

Results Table

The **Results** table displays the summary information for the Internet Server and Platform Server transfers that have been returned. After displaying summary information, you can click **Audit Id** to display detailed information about the selected transfer. You can also select Platform Transfers that can be resubmitted by selecting the **Resubmit** checkbox and then, clicking **Resubmit**. You can view the results of the resubmit in the **Resubmit Results** page.

Rights

The rights required to view audits are:

Right	Description
AdministratorRight	Allows you to view audit records.
ViewAuditRight	Allows you to view audit records.
HelpDeskRight	Allows you to view audit records.

Delegated Administration

Administration of audit records can be delegated to the users assigned to the department in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned a department or can manage the department can view transfers for their department or for any department that they can manage.

Note: Audit records created by a user not assigned to a department can be viewed by users with the required rights that are not assigned to a department.

Searching for Audits

To search for audits, complete the following steps.

Procedure

1. Click **Search Audits**.
2. Enter the required information.
3. When you have finished entering the information, click the **Search** button.

Viewing Audit Detail Information

To view the detailed information for a transfer, click the **Audit Id** from the **Search Criteria Results** table. The **Audit Details** page is displayed.

Deleting Audits

As an administrator, you can delete audit records from the database. You can delete audit records older than a particular date or define the number of days to save. We generally suggest using the scheduler **Purge DB Tables** job to delete audit records rather than using this page.

Rights

The rights required to view audits are:

Right	Description
AdministratorRight	Allows you to delete audit records.
DeleteAuditRight	Allows you to delete audit records.

Delegated Administration

Administration of deleting audit records can be delegated to the users with the required rights that are not assigned to a department.

Deleting an Audit

To delete an audit, complete the following steps.

Procedure

1. Click **Delete Audits**.
2. Enter the required information.
3. When you have finished entering the information, click the **Delete** button on the upper-right side of the page.
4. When prompted, click **OK**.

Audit Search Filters

As an administrator, you can define and search common search filters that can be used in the Search Audits page. Once you have created a search filter, you can select this filter in the **Search Audits > Selection Criteria > Retrieve pre-selected filter**.

Rights

The rights required to view audit search filters are:

Right	Description
AdministratorRight	Allows you to view and update audit search filters.
ViewAuditRight	Allows you to view and update audit search filters.
HelpDeskRight	Allows you to view and update audit search filters.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights assigned to a department.

> **Note:** When you are assigned to a department, the **Department box** is filled in with your department information. You can use this department or any department that you can manage.

Adding Audit Search Filters

The TIBCO MFT Server allows you to add a new audit search filter. The audit search filter information can be entered on this page. To add a new audit search filter, complete the following steps.

Procedure

1. Click **Add Audit Search Filter**.
2. Enter the required information in the **Audit Search Filter Selection Criteria** tab.
3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing Audit Search Filters

The **Manage Audit Search Filters** page displays the audit search filters that you are authorized to access. allows you to select an entry from the Audit Search Filters and update the settings of that entry.

Executing an Audit Search Filter

To execute an Audit Search Filter, complete the following steps.

Procedure

1. Go to **Reports > Audits > Search Audits**.

   The **Update Audit Search Filter** page is displayed.
2. Select the filter entry from the retrieve pre-selected filter within the **Search Criteria**.

There are two options to manage transfers:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the audit search filters to limit the number of definitions that are displayed in the **Results** table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before an audit search filter is returned. When you have completed the **Search Criteria**, click **Search** button to perform the search and create the **Results** table.

Results Table

Up to 100 audit search filters are displayed within the **Results** table. If you click the search audit ID of one of the entries in this table, the **Search Filter** page is displayed that also allows you to update the entry if you are authorized. The Search Audit result table page displays 100 to 1000 records based on the **Max Records Displayed Per Page** parameter specified in the search criteria. If the records exceed the defined value, you can view the next 100 to 1000 entries by clicking **Next**.

Updating Audit Search Filter Information

To update an audit search filter information, complete the following steps.

Procedure

1. Click the existing **Search Audit Id** from the **Results Table**.
2. Enter the required changes.
3. Click **Update**.

To return to the transfers list, click **Back to Audit Search Filter List**.

Deleting an Audit Search Filter

To delete an audit search filter, complete the following steps.

Procedure

1. Select the checkbox next to the audit search filter that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK.**

Statistics

As an administrator, you can display Internet Server and Platform Server transfer statistics in a variety of ways. The following table lists the various ways the statistics are displayed. The following criteria are set in the Search criteria:

Criteria	Description
Host	Internet Server host that transfers executed on (Internet Server transfers) or the Command Center host that collected the Platform Server transfer.
Server	For Internet Server transfers, the server definition that was the destination server for the transfers. For Platform Server transfers, Platform transfers collected from the defined server definition.
Interval	Daily, Weekly (A 7-day period that ends on the **End Date**) or Monthly (for the month defined by **Month**).
End Date	Defines the end data for the statistics.
Month	Defines the month when the interval is defined as `Monthly`.

Rights

The rights required to view statistics are:

Right	Description
AdministratorRight	Allows you to view transfer statistics.
ViewAuditRight	Allows you to view transfer statistics.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned a department.

Viewing Statistics

To view the statistics, complete the following steps.

Procedure

1. Enter the required information in the **Search Criteria**.
2. Click **Search**.

Management

As an administrator, you can manage MFT resources. The **Management** pages support the functions listed in the table below:

Function	Description
Protocol Keys	Allows you to define protocol system keys and associate protocol public keys with users and servers.
PGP Keys	Allows you to define PGP system keys and associate PGP public keys with users and servers.

Function	Description
SSH Algorithm Group	Allows you to define SSH key exchange algorithms, ciphers, hashes, and public Key algorithms to be used in incoming and outgoing SSH requests.

Protocol Keys

Protocol keys allow you to manage all keys used in file transfer protocols. The types of protocol keys are listed below:

- Public Keys
- System Keys
- Kerberos Keytabs
- Trusted Certificates

Public Keys

As an administrator, you can use asymmetric encryption public keys. In asymmetric encryption, data is encrypted with a public key and can be decrypted only if you have the private key and private key passphrase associated with the public key. Public keys are literally "public" in that they contain no secure information and can be distributed without security concerns. MFT uses public keys for the following purposes:

- User public keys are used for incoming key or certificate authentication. They equate an incoming public key to a user ID.
- Server public keys are used to validate connections to secure target servers.

Rights

The rights required to add, delete, list, and update protocol public keys.

Right	Description
AdministratorRight	Allows you to add, delete, list, and update Protocol Public Keys.
UpdatePublicKey	Allows you to add, delete, list, and update Protocol Public Keys.
ViewPublicKey	Allows you to list and view Protocol Public Keys.

Tasks

There are two links displayed for public keys.

Task	Description
Add Key	Allows you to associate a public key with a user or server.
Manage Keys	Allows you to list and manage all public keys. You can define **Search Criteria** to display only public keys that match the criteria. Once a list of public keys is displayed, you can click **Type** and the **Update Public Key** page is displayed. You can also delete Protocol Public Keys from the **Manage Public Keys** page. From within the **Update Public Key** page, the following actions are performed: • Display details about the system key. • For SSH keys, display the public SSH key associated with the system key.

Delegated Administration

Administration can be delegated in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department or can manage this department.

> **Note:** Public keys can be managed for users and servers assigned to a department that the admin user can manage.

Adding Public Keys

As an administrator, you can add a new public key. The public key information can be entered on this page. To add a new public key, complete the following steps.

Procedure

1. Click **Add Key**.
2. Select the required **Public Key Type**.
3. Select the required user or server.
4. Enter the required information.
5. When you have finished entering the information, click the **Continue** button on the upper-right side of the page.
6. When the **Add Public Key Confirmation** page is displayed, click the **Continue** button.

Managing Public Keys

The **Manage Public Keys** page displays all the public keys defined in the TIBCO MFT server. It also gives you the capability to search public keys to limit the number of public keys displayed. There are two options to manage public keys:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the public key to limit the number of records that are displayed on the public key results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 public key records are displayed within the **Results** table. If you click the **Type** of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Public Key Information

To update an existing public key information, complete the following steps.

Procedure

1. Click the type of a public key name from the **Results Table**.

   The **Update Public Key** page is displayed
2. Enter the required changes.
3. Click **Update**.

Deleting a Public Key

To delete a public key, complete the following steps.

Procedure

1. Select the checkbox next to the public key that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

System Keys

As an administrator, you can use system keys along with public keys for asymmetric encryption. System keys are secured by a passphrase. Without the passphrase, the system key cannot be used.

Important: Since system keys (sometimes referred to as private keys) are used to decrypt data, system keys, and system key passwords should be securely stored and should not be shared with anyone.

The system keys are used:

- By the transfer services: AS2, SFTP, FTPS, Platform Server, OFTP2, and HTTPS servers
- By SAML Single SignOn
- For key or certificate authentication when connecting to target SSH, FTPS, HTTPS, OFTP2, and Platform Servers.

Rights

The rights required to add, import, delete, list, and update protocol system keys are listed in the following table.

Right	Description
AdministratorRight	Allows you to add, import, delete, list, and update Protocol System Keys.
UpdateSystemKeyRight	Allows you to add, import, delete, list, and update Protocol System Keys

Tasks

There are three links displayed for public keys.

Task	Description
Create Key	Allows you to create a protocol system key.
Import Key	Allows you to create a system key from a file.
Manage Keys	Allows you to list and manage all system keys. You can define **Search Criteria** to display only system keys that match the criteria. Once a list of system keys is displayed, you can click **Type** and the **Update System Key** page is displayed. You can also delete Protocol Public Keys from the **Manage System Keys** page.

Delegated Administration

Administration can be delegated to users with the required rights that are not assigned to a department.

Creating Keys

As an administrator, you can create a new system key. The system key information can be entered on this page. To create a new system key, complete the following steps.

Procedure

1. Click **Create Key**.
2. Enter the required information.
3. When you have finished entering the information, click the **Create Key** button on the upper-right side of the page.

Importing Keys

As an administrator, you can import a system key. To import a system key, complete the following steps.

Procedure

1. Click **Import Key**.
2. Enter the required information.
3. When you have finished entering the information, click the **Import Key** button on the upper-right side of the page.

   A confirmation page is displayed.
4. Click **Continue** after verifying the information on the confirmation page.

Managing Keys

The **Manage Keys** page displays the first 100 system key records defined in the TIBCO MFT server. It also gives you the capability to search the system key record database to limit the number of system key records displayed. There are two options to manage system keys:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the system key record database to limit the number of records that are displayed on the system key results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 user records are displayed within the **Results** table. If you click the **Description** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Key Information

To update an existing system key information, complete the following steps.

Procedure

1. Click the existing description from the **Results Table**.

   The **Update System Key** page is displayed.

2. Click the required button as described in the following table.

Button	Description
Back to Search	Return to the **Manage System keys** page.
Disable Key	Disable the key if it is enabled.

Button	Description
Enable Key	Enable the key if it is disabled
Set as Default	Set as the default key.
Export	Export the key to a file.

Deleting a Key

To delete a system key, complete the following steps.

Procedure

1. Select the checkbox next to the key that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

Kerberos Keytabs

As an administrator, you can use Kerberos keytabs for communicating to target HDFS servers when the server is configured for Kerberos authentication.

Rights

The rights required to add, import, delete, list, and update kerberos keytabs are listed in the following table.

Right	Description
AdministratorRight	Allows you to add, delete, list, and update Kerberos keytabs.
UpdateSystemKeyRight	Allows you to add, delete, list, and update Kerberos keytabs.

Tasks

There are two links displayed for public keys.

Task	Description
Import KeyTab	Allows you to import a Kerberos keytab
Manage KeyTabs	Allows you to list, update, and delete Kerberos keytabs. The **Update KeyTab** option allows you to enable or disable keytabs, and set a keytab as the default keytab.

Delegated Administration

Administration can be delegated to users with the required rights that are not assigned to a department.

Importing Keytabs

As an administrator, you can import a keytab. The keytab information can be entered on this page. To import a keytab, complete the following steps.

Procedure

1. Click **Import KeyTab**.
2. Enter the required information.
3. When you have finished entering the information, click the **Import Key** button on the upper-right side of the page.

Managing Keytabs

The **Manage KeyTabs** page displays the first 100 keytab records defined in the TIBCO MFT server. It also gives you the capability to search the keytab record database to limit the number of keytab records displayed. There are two options to manage keytab:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the database to limit the number of records that are displayed on the keytab results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 keytabs are displayed within the **Results** table. If you click the keytab ID of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized.

Updating Key Information

To update an existing keytab information, complete the following steps.

Procedure

1. Click the Description from the **Results Table**.

   The **Update KeyTab** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Key

To delete a keytab, complete the following steps.

Procedure

1. Select the checkbox next to the keytab that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

Trusted Certificates

As an administrator, you can utilize the **Trusted Certificates** page for the following purposes:

- Simplifies incoming certificate authentication. If many clients use system keys signed by the same certificate authority, you can add the CA certificate as a trusted certificate. Then, you can define the user record: Authentication Options: Certificate DN with the distinguished name of the certificate. When an incoming request is detected, MFT will search for a trusted certificate match on the incoming certificate. If a match is found, we will compare the certificate DN to the DN defined by the user record.
- When connecting to certain FTP Servers (z/OS, for example), the FTP client needs to pass a list of certificates to the FTP server. The FTP server will verify that their private key is supported by the client. To do this, you must save the FTP server certificate as a trusted certificate and set the web.xml **SendMFTTrustedCerts** option to `True`.

Rights

The rights required to add, import, delete, list, and update protocol trusted certificates are listed in the following table.

Right	Description
AdministratorRight	Allows you to add, delete, list, and update trusted certificates.
UpdatePublicKeyRight	Allows you to add, delete, list, and update Protocol Trusted Certificates.
ViewPublicKeyRight	Allows you to list and view Protocol Trusted Certificates.

Tasks

There are two links displayed for trusted certificates.

Task	Description
Add Trusted Certificate	Allows you to add a trusted certificate.
Manage Trusted Certificates	Allows you to list, update, and delete trusted certificates.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to a department.

Adding Trusted Certificate

As an administrator, you can add a new trusted certificate. To add a new trusted certificate, complete the following steps.

Procedure

1. Click **Add Trusted Certificate**.
2. Enter the required information.
3. When you have finished entering the information, click the **Continue** button on the upper-right side of the page.

Managing Trusted Certificates

The **Manage Trusted Certificates** page displays all the public keys defined in the TIBCO MFT server. It also gives you the capability to search trusted certificates to limit the number of trusted certificates displayed. There are two options to manage trusted certificates:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the trusted certificates to limit the number of records that are displayed on the trusted certificates results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 trusted certificate records are displayed within the **Results** table. If you click the **Trusted Certificate Name** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating Trusted Certificate Information

To update an existing trusted certificate information, complete the following steps.

Procedure

1. Click the **Certificate Type** from the **Results Table**.

   The **Update Trusted Certificate** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Trusted Certificate

To delete a trusted certificate, complete the following steps.

Procedure

1. Select the checkbox next to the trusted certificate that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

PGP Keys

PGP keys allow you to manage all PGP keys used in file transfer protocols. PGP is used to encrypt or decrypt, compress or decompress, and optionally sign or verify data that is transferred. Encrypting data secures the transmission of the data. Signing the data provides non-repudiation of the data.

Data is encrypted using the PGP public key of the transfer partner. Only a user with the PGP system key and system key password associated with the PGP public key can decrypt the data.

Data is signed with the PGP system key. Any user that has the PGP public key can verify the signature of the data, and therefore, the system that encrypted and signed the data.

Encrypt or Decrypt Data

MFT Internet Server can encrypt or decrypt data in the following ways:

Transfer client sends (that is, uploads) an encrypted file. MFT Internet Server decrypts and decompresses the data as it is received from the partner. After all data is received, MFT Internet Server can optionally verify the signature of the data. In this case, the transfer definition defines whether the incoming data must be PGP decrypted, decompressed, and whether the data signature should be verified.

Transfer client receives (that is, downloads) an encrypted file from MFT Internet Server. MFT Internet Server encrypts and compresses the data as it is sent to the transfer client. After all data is sent, MFT Internet Server signs the data. In this case, the transfer definition defines whether the outgoing data must be PGP encrypted, compressed, and signed.

MFT Internet Server sends encrypted data to a target server. MFT Internet Server will encrypt and compress the data as it is sent to the target server. After all data is sent, MFT Internet Server will optionally sign the data. In this case, the Server definition defines whether the outgoing data must be PGP encrypted, compressed, and signed.

MFT Internet Server receives encrypted data from the target server. MFT Internet Server will decrypt and decompress the data as it is received from the target transfer server. After all data is received, MFT Internet Server will optionally verify the signature. In this case, the Server definition defines whether the incoming data must be PGP decrypted, decompressed, and verified.

There are two types of PGP keys:

- Public Keys
- System Keys

PGP Public Keys

As an administrator, you can use PGP public keys to encrypt data and to verify the signature of signed data. In PGP encryption, data is encrypted with a PGP public key and can be decrypted only if you have the PGP private key and PGP private key passphrase associated with the PGP public key. PGP public keys are literally "public" in that they contain no secure information and can be distributed without security concerns. MFT uses public keys for the following purposes:

- User PGP public keys are used to encrypt data and verify data signed by transfer clients. They equate a PGP public key to a User ID.
- Server PGP public keys are used to encrypt data and verify data signed by transfer servers. They equate a PGP public key to a target server.

Rights

The rights required to add, delete, list, and update PGP public keys.

Right	Description
AdministratorRight	Allows you to add, delete, list, and update PGP Public Keys.
UpdatePGPPublicKeyRight	Allows you to add, delete, list, and update PGP Public Keys.
ViewPGPPublicKeyRight	Allows you to list and view PGP Public Keys.

Tasks

There are two links displayed for PGP public keys.

Task	Description
Add Key	Allows you to associate a PGP public key with a user or server.
Manage Keys	Allows you to list and manage all PGP public keys. You can define **Search Criteria** to display only PGP public keys that match the criteria. Once a list of PGP public keys is displayed, you can click **Type** and the **Update PGP Public Key** page is displayed. You can also delete PGP Public Keys from the **Manage PGP Public Keys** page.

Delegated Administration

Administration can be delegated in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to this department.

> **Note:** PGP keys can be managed for users and servers assigned to a department that the admin user can manage.

Adding PGP Keys

As an administrator, you can add a new PGP public key. The PGP public key information can be entered on this page. To add a new PGP public key, complete the following steps.

Procedure

1. Click **Add PGP Public Key**.
2. Enter the required information.
3. Define whether the key is for a user or a server.
4. Select the required user or server.
5. When you have finished entering the information, click the **Continue** button on the upper-right side of the page.
6. When the **Add PGP Public Key Confirmation** page is displayed, click the **Continue** button.

Creating PGP Keys

As an administrator, you can create a new PGP system key. The PGP system key information can be entered on this page. To create a new PGP system key, complete the following steps.

Procedure

1. Click **Create PGP Key**.
2. Enter the required information.
3. When you have finished entering the information, click the **Create Key** button on the upper-right side of the page.

Managing PGP Public Keys

The **Manage PGP Public Keys** page displays all the public keys defined in the TIBCO MFT server. It also gives you the capability to search PGP public keys to limit the number of PGP public keys displayed. There are two options to manage PGP public keys:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the PGP public keys to limit the number of records that are displayed on the PGP public key results table. The percent sign (%) is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering is done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record is returned. When you have completed the **Search Criteria**, click **Search** to perform the search and create the **Results** table.

Results Table

Up to 100 PGP public key records are displayed within the **Results** table. If you click the **PGP Public Key Name** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating PGP Public Key Information

To update an existing PGP public key information, complete the following steps.

Procedure

1. Click the existing PGP public key name from the **Results Table**.

   The **Update PGP Public Key** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a PGP Public Key

To delete a PGP public key, complete the following steps.

Procedure

1. Select the checkbox next to the PGP public key that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

System Keys

As an administrator, you can use PGP system keys along with PGP public keys for decrypting and signing data. PGP system keys are secured by a passphrase. Without the passphrase, the PGP system key cannot be used.

Important: Since PGP system keys (sometimes referred to as private keys) are used to decrypt data, system keys, and system key passwords must be securely stored and must NOT be shared with anyone.

System keys are used for the following purposes:

- Decrypting Data
- Signing data

Rights

The rights required to add, delete, list, and update PGP public keys.

Right	Description
AdministratorRight	Allows you to add, delete, list, and update PGP System Keys.
UpdatePGPSystemKeyRight	Allows you to create, import, delete, list, and update PGP System Keys.

Tasks

There are three links displayed for PGP system keys.

Task	Description
Create PGP Key	Allows you to create a PGP system key.
Import PGP Key	Allows you to import system keys.
Manage PGP Keys	Allows you to list all PGP system keys. You can define **Search Criteria** to display only PGP system keys that match the criteria. Once a list of PGP system keys is displayed, you can click **Description** and the **Update PGP System Key** page is displayed. From within the **Manage PGP System Keys** page, you can do the following tasks: • Display details about the PGP system key. • Display the PGP public key associated with the PGP system key. • Enable or disable the PGP system key. • Set the PGP system key as the default PGP system key. You can also delete PGP system keys in the Manage PGP system keys page.

Delegated Administration

Administration can be delegated to users with the required rights that are not assigned to a department.

Creating Keys

As an administrator, you can create a new system key. The system key information can be entered on this page. To create a new system key, complete the following steps.

Procedure

1. Click **Create Key**.
2. Enter the required information.
3. When you have finished entering the information, click the **Create Key** button on the upper-right side of the page.

Importing PGP Keys

As an administrator, you can import a system PGP key. To import a PGP system key, complete the following steps.

Procedure

1. Click **Import PGP Key**.
2. Enter the required information.
3. When you have finished entering the information, click the **Continue** button on the upper-right side of the page.
4. When a confirmation page is displayed, click the **Continue** button.

Managing PGP System Keys

The **Manage PGP System Keys** page displays all the PGP system keys defined in the TIBCO MFT server. It also gives you the capability to search PGP system keys to limit the number of PGP system keys displayed. The PGP system keys are displayed in the **Results** table.

Results Table

Up to 100 PGP system key records are displayed within the **Results** table. If you click the **Description** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking **Next**.

Updating PGP System Key Information

To update an existing PGP system key information, complete the following steps.

Procedure

1. Click the PGP system key description from the **Results Table**.

   The **Update PGP System Key** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a PGP System Key

To delete a PGP system key, complete the following steps.

Procedure

1. Select the checkbox next to the PGP system key that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

SSH Algorithm Groups

SSH algorithm groups allow you to define groups of SSH Key Exchange Algorithms, Ciphers, Hashes (Message Digests), and Public key algorithms. You can then assign the SSH Groups to server definitions or to the SSH Service. You can also select an SSH algorithm group on the **System Configuration > SSH Settings** page to make this Algorithm Group the default for all MFT instances. The **Add SSH Algorithm Group** page allows you to create an SSH algorithm group, while the **Update SSH Algorithm Group** page allows you to modify an existing SSH algorithm group.

Rights

The **AdministratorRight** right is required to add, delete, list, and update SSH algorithm keys.

Tasks

There are two links displayed for SSH algorithm keys.

Task	Description
Add Algorithm Group	Allows you to create a new SSH algorithm group definition.
Manage Algorithm Group	Allows you to list and manage all SSH algorithm groups.

Delegated Administration

Administration can be delegated to SSH algorithm groups with the required rights that are not assigned to a department.

Adding Algorithm Groups

As an administrator, you can add a new SSH algorithm group. To add a new SSH algorithm group, complete the following steps.

Procedure

1. Click **Add SSH Algorithm Group**.
2. Enter the required information.
3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Note: You can retrieve the SSH algorithms supported by an Internet Server instance by selecting a server and clicking the **Retrieve Algorithms** from this Internet Server button. This fills in the **Available Algorithms** boxes. You can select the algorithms and drag them to the **Selected Algorithms** box. If you click **All >>**, all algorithms are copied to the **Selected Algorithms** box.

Managing SSH Algorithm Groups

The Manage SSH Algorithms page lists all configured SSH algorithm groups. Each defined algorithm group is displayed in the **Results** table.

Result

This box lists all SSH algorithm groups that have been defined. Click the **Name** of an algorithm group to display the Update SSH Algorithm Group page.

Updating SSH Algorithm Groups

To update SSH algorithm groups, complete the following steps.

Procedure

1. From the **Manage SSH Algorithm Groups** page, click the **Algorithm Name**.

   The **Update SSH Algorithm Group** page is displayed.
2. Enter the required information.
3. When you have finished entering the information, click the **Update** button on the upper-right side of the page.

Configuration

As an administrator, you can configure various MFT functions. The following table lists functions are included under **Configuration.**

Function	Description
System Configuration	Update System Configuration.
FileShare	Update FileShare Configuration.
Single SignOn	Update SAML and OIDC (OpenID Connect) configuration.

Function	Description
Multi Factor Authentication	Allows you to define multi-factor authentication for browser logons.
Admin Changes	Allows you to view admin changes that have occurred.
Authenticators	Allows you to add, manage, and update LDAP Authenticators.

System Configuration

As an administrator, you can display and update global configuration parameters.

Rights

The **AdministratorRight** is required to view and update the system configuration.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Updating System Configuration

As an administrator, you can update system configuration. The system configuration information can be entered on this page. To update system configuration, complete the following steps.

Procedure

1. Click **System Configuration**.
2. Enter the required information described in the table below:

Note: Each tab of the **System Configuration** page has an **Update** button. Each tab is updated individually; only the parameters on the current tab are updated when you click the **Update** button.

Tab	Description
Global Settings	Defines the following: • Email Server Information • Email Template Settings • LDAP Settings for the LDAP Sync Server • Miscellaneous settings
Server Settings	Defines parameters specific to individual Internet Server and Command Center hosts in the MFT Cluster. To view and update parameters for a specific host, you must first select the host. Parameters that can be updated include: • Connectivity information to that server • Tracing settings • Other miscellaneous settings
Password Reset and Self Registration Rules	Defines various parameters for **Password Reset** and **Self Registration**.
Password Rules	Defines the password rules that will be enforced when a user changes their password or when an admin changes the user password.
Lockout Rules	Defines lockout runs for invalid log in attempts. These parameters are displayed and can be updated. • Log in Failure Attempts

Tab	Description
	• Failure Retention Period • Lock Action • Lock Duration • Lockout Exclusion Settings
ReCaptcha Settings	Allows you to enable ReCaptcha for MFT log in, forgot user, forgot password, and self-register pages.
Antivirus Settings	Allows you to enable and configure antivirus checking.
Default Config Settings	Defines the default settings for a variety of administrative settings: • Internet Server Transfer Definitions • Platform Server Transfer Definitions • User Definitions • Protocol System Key Definitions • PGP System Key Definitions
Transfer Settings	Defines upload and download REGEX rules to globally restrict uploads and downloads.
PGP Settings	Defines default values for PGP settings. In most cases, these parameter defaults are related to configuring PGP System Keys and adding PGP keys. Parameter "Strict private key decryption only" defines whether any PGP System Key can be used to decrypt data, or whether only PGP System Keys assigned to Server and Transfer definitions can be used to decrypt data.
FTP Settings	Defines parameters used by the Internet Server FTP server and FTP client. It allows you to specify the ports to be used for data connections. It also defines rules about users adding their own

Tab	Description
	FTP public keys. Most importantly, it defines how users will authenticate to the MFT Internet Server FTP server and whether certificates or passwords are required.
SSH Settings	Defines parameters used by the Internet Server SSH server. It also defines rules about users adding their own SSH public keys. Most importantly, it defines how users will authenticate to the MFT Internet Server SSH Server and whether keys and certificates or passwords are required.
HTTPS Settings	Defines how users will authenticate to the MFT Internet Server HTTPS Server and whether certificates or passwords will be required. **Note:** You must also configure the HTTPS connector in the `server.xml` file to enable HTTPS certificate authentication.
Platform Server Settings	Defines how users will authenticate to the MFT Internet Server Platform Server service: whether certificates or passwords are required. **Note:** This setting is only used for incoming Platform Server SSL or TLS and Platform Server tunnel requests.
Data Loss Prevention Settings	Allows you to enable and configure DLP scanning.

3. When you have finished entering the information, click the **Update** button.

FileShare Configuration

The **File Share Configuration** page allows you to configure the FileShare server. Fields on this page are broken up into common sections. Fields prefixed with a red "*" are required fields and must be entered. Other fields can be entered when necessary.

Rights

The **AdministratorRight** is required to view and update the FileShare configuration.

Delegated Administration

Administration can be delegated only to super administrators.

> **Note:** A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Updating FileShare Configuration

As an administrator, you can update FileShare configuration. The FileShare configuration information can be entered on this page. To update the FileShare configuration, complete the following steps.

Procedure

1. Click **FileShare > Configuration**.
2. Enter the required information.
3. When you have finished entering the information, click the **Update** button on the upper-right corner of the page.

Archive Server Status

As an administrator, you can remove deleted and old revisions of FileShare files and folders. You can also remove expired mailbox requests and delete mailbox attachments. The following table lists the functions the **Archive Server Status** page performs.

Function	Description
Server Status	Gets the status of the Archive server.

Function	Description
Start Server	Starts the Archive server.
Stop Server	Stops the Archive server.

Single SignOn

The **Single SignOn** pages allows you to configure single sign-on for HTTP login requests. The **Single SignOn** requests only apply to HTTP or HTTPS password authentication requests. It does not apply to other protocols such as FTP, SFTP, or Platform Server. It does not apply when an HTTPS client logs on using certificate authentication.

Two types of single sign-on are supported:

- OpenID Connect (OIDC)
- SAML

OpenID Connect is simpler than SAML to configure and use. We recommend using OpenID Connect for single sign-on when possible.

OpenID Connect

OpenID Connect, commonly known as OIDC, is a single sign-on standard built on top of OAUTH2. It allows a third party called the Identity Provider, to authenticate users and send secure tokens to the application (Internet Server and Command Center) to be used to log in users.

Rights

The **AdministratorRight** is required to view and update the OpenID Connect Configuration.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Adding OIDC Provider Configuration

As an administrator, you can add OIDC provider configuration. The OIDC provider configuration information can be entered on this page. To update OIDC provider configuration, complete the following steps.

Procedure

1. Click **Add OIDC Provider Configuration**.
2. Enter the required information.
3. When you have finished entering the information, click the **Add** button on the upper-right corner of the page.

Managing OIDC Provider Configurations

The **Manage OIDC Provider Configurations** page displays all the OIDC provider configurations defined in the TIBCO MFT server. OIDC providers are servers that authenticate users and return the encrypted and signed authentication assertions to Internet Server and Command Center. It also gives you the capability to search OIDC provider configurations to limit the number of OIDC provider configurations displayed. The OIDC provider configurations are managed by the **Results** table.

Results Table

All OIDC provider configuration records are displayed within the **Results** table. If you click the **Name** of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized.

Updating OIDC Provider Configurations

To update an existing OIDC provider configuration, complete the following steps.

Procedure

1. Click the **Name** from the **Results** Table.

   The **Update OIDC Provider Configuration** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Managing MFT OIDC Instances

The **Manage MFT OIDC Instances** page displays all MFT Internet Server and Command Center instances that can be configured for **OIDC Single SignOn**. All of the Internet Server and Command Center instances, along with the default templates are displayed in the **Results** Table.

Results Table

This box lists all MFT OIDC Instances that have been defined. Click the **Host Name** of an OIDC Instance to display the **Update MFT OIDC Instance** page.

All MFT OIDC instances are displayed within the **Results** table. If you click the **Host Name** of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized.

Updating MFT OIDC Instances

To update an existing MFT OIDC instance, complete the following steps.

Procedure

1. Click the **Host Name** from the **Results** Table.

   The **Update MFT OIDC Instance** page is displayed.
2. Enter the required changes.
3. Click **Update**.

SAML Configuration

SAML, also known as Secure Assertion Markup Language, is a standard for exchanging authentication data between a SAML Identity Provider and a Service Provider (Internet

Server and Command Center). It performs single sign-on for the HTTP/HTTPS protocols.

As an administrator, you can configure SAML Single Sign-On. The following functions must be performed to configure **SAML Single SignOn**:

- Import SAML IDP Metadata
- Configure SAML SP Metadata
- Generate SAML SP Metadata

Rights

The **AdministratorRight** is required to view and update the SAML configuration.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Importing SAML IDP MetaData

As an administrator, you can list all Internet Server and Command Center instances. You must select the server to display the page for that server.

The SAML IDP MetaData typically is generated by the SAML IDP and is sent to the MFT admin. You must copy or paste this information into the **Update MFT OIDC Instance** page.

Procedure

1. Click **Import SAML IDP MetaData**.
2. Enter the required information.
3. When you have finished entering the information, click the **Import** button on the upper-right side of the page.

Configuring SAML SP MetaData

As an administrator, you can configure an SAML SP metadata. To configure an SAML SP metadata, complete the following steps. SAML MetaData includes the following information:

- Service Provider ID
- The SAML attribute that contains the User ID
- Defines whether to encrypt and sign SAML messages
- Defines the private keys used for SAML encryption and signing
- Defines the authenticators that should be checked for incoming SAML requests

Procedure

1. Click **Configure SAML SP MetaData**.
2. Enter the required information.
3. When you have finished entering the information, click the **Update** button on the upper-right side of the page.

Generating SAML SP MetaData

As an administrator, you can import an SAML SP metadata. To import an SAML SP metadata, complete the following steps.

Procedure

1. Click **Generate SAML SP MetaData**.
2. Enter the required information.
3. When you have finished entering the information, click the **Generate** button.

   After generating the SAML SP MetaData, you typically send this information to SAML Admin.

Multi-Factor Authentication

MFT supports two Multi-Factor Authentication(MFA) methods:

- Email
- Google Authenticator

For information on how to configure MFA on some or all instances, see the following topics.

Common MFA Configuration

This page allows you to define Multi-Factor Authentication (MFA) configuration parameters common to all MFT instances.

Rights

`AdministratorRight` is required to view and update the common MFA configuration.

Updating Common Multi-Factor Authentication (MFA) Configuration

As an administrator, you can update Email MFA parameters, Google MFA parameters, and parameters that are common to all the MFA methods on this page. To update the configuration, complete the following steps.

Procedure

1. Click **Common MFA Configuration**.
2. To enable Email MFA, update the applicable Email MFA parameters.
3. To enable Google Authenticator MFA, update the applicable Google MFA parameters.
4. Update the common MFA parameters applicable for all the MFA methods.
5. Click **Update** on the top-right corner of the screen.

Manage MFT MFA Instances

The Manage MFT MFA Instances page displays all MFT Internet Server and Command Center instances that can be configured for Multi-Factor Authentication. All the Internet Server and Command Center instances, along with the default templates are displayed in the **Results** table.

Results Table

This box lists all MFT MFA Instances that have been defined. Click the **Host Name** of an MFT MFA Instance to display the Update MFT MFA Instance page.

All MFT MFA instances are displayed within the **Results** table. If you click the **Host Name** of one of the entries in this table, a detailed page is displayed that allows you to update the entry if you are authorized.

Updating MFT MFA Instance

To update an MFT MFA Instance, complete the following steps:

Procedure

1. Click the Host Name from the results table.
2. Enable or Disable the Email or Google MFA on the Update MFT MFA Instance page for the selected Host.
3. Click update on the top right corner.

Admin Changes

As an administrator, you can define search for and display details on all administrator changes made. MFT Tracks the following admin changes:

- All changes to the configuration through the admin pages, the Command Line utility and REST calls.
- Starting and stopping the MFT server.
- Starting and stopping the MFT Services (ex: SSH Service, FTP Service…).

When this page starts, all changes made on the current date are displayed in the results table. Additionally, you can use the **Search Criteria** to filter changes to be displayed.

Rights

The rights required to view admin changes.

Right	Description
AdministratorRight	Allows you to view admin changes.
ViewPCILogRight	Allows you to view admin changes.

Tasks

The following task is displayed for admin changes:

Task	Description
View Admin Changes	Allows you to view admin changes.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to a department. Only changes for departments that the user can manage will be displayed.

Viewing Admin Changes

On the **Search Admin Changes** page, all changes made today are displayed. You can set the **Search Criteria** to define the changes and the date range to be displayed.

The **Results** table displays summary information on the changes. Click the **ID** field to get detailed information about the change.

You can click the **ID** field in the **Results** table to display detailed information about the admin change request. This page displays information about the change, including when the change was made, the User ID that made the change and the IP Address of the user that made the change. It also displays information about the parameters that were changed.

Authenticators

As an administrator, you can add and display LDAP authenticators. LDAP authenticators allow you to define LDAP Servers that can be used when MFT clients connect to Internet Server or Command Center. When you define an LDAP authenticator, you must assign a **Name** to the authenticator. When you use the **Sync** option on the LDAP Authenticator, User IDs will be created with a user name in the following format: `AuthenticatorName-userid`

For example, if you have an authenticator called `AD` and the User ID synced is `User1`, the **MFT Userid** is `AD-User1`.

The LDAP Sync function is defined in the **Administration > LDAP Sync** page.

Rights

The `AdministratorRight` is required to view and update the LDAP authenticators.

Tasks

There are two links displayed for authenticators.

Task	Description
Add Authenticator	Allows you to create a new authenticator.
Manage Authenticators	Allows you to list, update, delete, and test authenticators. Once you list the authenticators, you can test, update, and delete authenticators.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Adding Authenticators

As an administrator, you can add a new authenticator. The authenticator user information can be entered on this page. To add a new authenticator, complete the following steps.

Procedure

1. Click **Add Authenticator**.
2. Enter the required information described in the table below:

<table>
<tr><th>Tab</th><th>Description</th></tr>
<tr><td>Authenticator</td><td>Defines the name of the authenticator, the authenticator type, and the servers that should use this authenticator. It also allows you to enable or disable the authenticator.</td></tr>
<tr><td>LDAP Connectivity</td><td>Defines the information necessary to connect to the LDAP server:
Host Name or URL and Port
Bind User DN and Password
Whether SSL is used when connecting to the LDAP server</td></tr>
<tr><td>LDAP Search</td><td><table><tr><th>Function</th><th>Properties</th></tr><tr><td>User Base DN</td><td>Defines where MFT users and groups are located in the LDAP tree.</td></tr><tr><td>Sync Group DN</td><td>Defines the fully qualified DN (Distinguished name) of the group that contains the users to sync.</td></tr><tr><td>Search Filter</td><td>Provides a more efficient method to search for MFT users to sync. Whenever possible, use this instead of the Sync Group DN. Using a search filter generally requires that the user object contains the list of groups a user is a member of. Active Directory and some newer versions of OpenLDAP</td></tr></table></td></tr>
</table>

<table>
<tr><th>Tab</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Function</th><th>Properties</th></tr>
<tr><td></td><td>support this.</td></tr>
<tr><td>Search Scope</td><td>Defines the scope of the search.</td></tr>
</table>
</td></tr>
<tr><td>LDAP User Attributes</td><td>Defines the LDAP user attributes that are used when syncing users. You can define LDAP user attributes for:
User Name
Full Name
Email Address
Phone Number
Department
Usage
User Type
Expiration Date
Visibility</td></tr>
<tr><td>Right Management</td><td>Defines whether user rights are synced when a user is synced.

To configure that all synced users be given TransferRight, select the checkbox next to Assign TransferRight to all users in this authenticator

To configure that a right should be synced, click Enable on the left checkbox and define a group name in the LDAP Group Name box.

Right Group Base DN: defined the default DN where right groups are located. This field is only used when the LDAP Group Name for</td></tr>
</table>

Tab	Description
	the individual rights does not contain an "=". If a synced right **LDAP Group Name** contains an "=", then the **LDAP Group Name** is a fully qualified group and the **Right Group Base DN** is ignored. If this **Right Group Base DN** is defined and a right is enabled and the **LDAP Group Name** does NOT contain a "=", MFT will search for groups in the DN defined by the **Right Group Base DN** **Rights:** Each right is listed. To enable right syncing, select the checkbox to the left of the **Right Name**. Then, specify either the name of the group in the **Right Group Base DN**, or the fully qualified DN of the group. Members of this group will be assigned the defined right.

3. When you have finished entering the information, click the **Add** button on the upper-right side of the page.

Managing Authenticators

The **Manage Authenticators** page displays all authenticator records defined in the TIBCO MFT server. It also gives you the capability to search the authenticator record database to limit the number of authenticator records displayed. You can manage authenticators using the **Results** table.

Results Table

All authenticator records are displayed within the **Results** table. If you click the **Authenticator Name**, the **Update Authenticator** page is displayed. If you click the test of one of the entries in this table, a detail page is displayed that allows you to update the entry if you are authorized.

Updating an Authenticator

To update an authenticator, complete the following steps.

Procedure

1. Select the checkbox next to the authenticator that you want to delete.
2. Click the update icon.
3. When prompted, click **OK**.

Deleting an Authenticator

To delete an authenticator, complete the following steps.

Procedure

1. Select the checkbox next to the authenticator that you want to delete.
2. Click the delete icon.
3. When prompted, click **OK**.

Administration

As an administrator, you can perform a variety of administrative functions for the MFT cluster. The following table lists functions that are included in the **Administration** page:

Function	Description
Transfer Servers	Configure and start status, stop status, or get status of Transfer Servers (that is, FTP, AS2, SFTP, OFTP2, and Platform Server).
LDAP Sync	Allows you to sync one or more LDAP authenticators or LDAP users with the MFT database.
Lockout Management	View and reset system, user and IP address lockouts.
Activity	Allows you to view and terminate active sessions. Also allows you to delete checkpoint records.
Active Transfers	Allows you to display active transfers across all Internet Server instances in the MFT Cluster.

Transfer Servers

As an administrator, you can perform these functions for AS2, FTP, SSH, and Platform Server services:

- Configure the server.
- Start, stop, and display the status of the server.

Transfer Servers are the MFT components that listen on TCP ports and wait for incoming file transfer requests.

Rights

The `AdministratorRight` is required to configure, start, stop, and display the server status.

Right	Description
AdministratorRight FTAdminRight UpdateTransferServiceRight	Allows you to list, view, delete, and update database user profiles records. However, you cannot retrieve or update user profile definitions on Platform Servers unless you also have `FTAdminRight`.
FTAdminRight ViewServerRight	Allows you to list, view, delete, and update database user profiles records. You can also retrieve, delete, and update user profile definitions on Platform Servers.
FTAdminRight	Allows you to list, view, delete, and update database user profiles records.

Tasks

There are two links displayed for Platform Server user profiles:

Task	Description
AS2 Server	Allows you to create a new platform server user profile.

Task	Description
FTP Server	Allows you to list and manage all platform server user profiles.
SSH Server	Allows you to configure, start, stop, and get status of the SSH server and the SFTP server.
OFTP2 Server	Allows you to configure, start, stop, and get status of the OFTP2 server.
Platform Server	Allows you to configure, start, stop, and get status of the Platform Server.
TIBCO Accelerator	Allows you to start, stop, and get status of the TIBCO Accelerator.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with `AdministratorRight` that is not assigned to a department.

AS2 Server: AS2 Server Status

As an administrator, you can start, stop, and display the status of the AS2 server on Internet Server instances. The following table lists the function you can perform on this page.

Function	Operation
Start	Starts the AS2 service.
Stop	Stops the AS2 service.
Server Status	Displays the status of the AS2 service.

AS2 Server: Configuring AS2 Server

As an administrator, you can configure the AS2 server for the Internet Server instances.

When this page is entered, you must select the server that you want to configure. The following information can be configured for the AS2 server:

Parameter	Description
Enabled	Whether the AS2 server is enabled.
Receive URL	Defines the URL that MFT IS uses for incoming requests.
Async Response URL	Defines the URL that MFT IS uses to receive asynchronous responses.
Local AS2 ID	Defines the default name of the AS2 instance. This name, if not overridden, must match the Partner AS2 ID configured on the partner AS2 system.
Proxy Information	Defines proxy information for outgoing AS2 requests.

Note: In addition to the entries for each Internet Server, an entry is also displayed called ***DefaultTemplate**. This entry is used when running Internet Server in the cloud and instances are started and stopped dynamically. The default template provides the default configuration for instances started dynamically.

FTP Server: FTP Server Status

As an administrator, you can start, stop, and display the status of the FTP server on Internet Server instances. The following table lists the functions you can perform on this page.

Function	Operation
Start	Starts the FTP service.
Stop	Stops the FTP service.
Server Status	Displays the status of the FTP service.

Note: When you stop or start the FTP server on an Internet Server instance, both FTP services (clear text and SSL) are stopped or started.

FTP Server: Configure FTP Server

As an administrator, you can configure the FTP server for the Internet Server instances. When this page is entered, you must select the server that you want to configure. The following information can be configured for the FTP server:

Parameter	Description
Enabled	Whether the FTP server is enabled.
IP Port	Defines the ports that the FTP servers listen on for clear and explicit SSL connections.
SSL Port	Defines the ports that the FTP servers listens on for Implicit SSL connections.
Bind Adapter IPV4 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
Bind Adapter IPV6 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
FTP System Key	Defines the system key used for SSL or TLS services
Welcome	Defines the message that is displayed when you log in to the MFT FTP

Parameter	Description
Message	Server.
External IP Address	Defines the IP address used under these circumstances: • An FTP client initiates a PASV request. • MFT issues a PORT request to a target FTP server. This IP Address is used when an Internet Server data connection listens on an IP address and notifies the FTP partner of the IP Address and port that should be used to connect back to this port.
Miscellaneous parameters	There are a variety of other configuration parameters allowed for the FTP server.

Note: In addition to the entries for each Internet Server, an entry is also displayed called ***DefaultTemplate**. This entry is used when running Internet Server in the cloud and instances are started and stopped dynamically. The default template provides the default configuration for instances started dynamically.

Platform Server: Platform Server Status

As an administrator, you can start, stop, and display the status of the Platform Server on Internet Server instances. The following table lists the function you can perform on this page.

Function	Operation
Start	Starts the Platform Server service.
Stop	Stops the Platform Server service.
Server Status	Displays the status of the Platform Server service.

Platform Server: Configure Platform Server

As an administrator, you can configure the Platform Server for the Internet Server instances. When this page is entered, you must select the server that you want to configure. The following information can be configured for the Platform Server:

Parameter	Description
Enabled	Whether the Platform Server service is enabled.
IP Port	Defines the ports that the Platform Server service listens on for standard Platform Server requests.
SSL IP Port	Defines the ports that the Platform Server service listens on for SSL or TLS Platform Server requests
TLS Tunnel Port	Defines the ports that the Platform Server service listens on for TLS tunnel Platform Server requests.
SSL System Key	Defines the system key used for SSL and TLS tunnel requests.
Bind Adapter IPV4 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
Bind Adapter IPV6 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
SocketTimeout	Defines the time that a **TCP Send** or **Receive** request will wait for completion before it times out.

Note: In addition to the entries for each Internet Server, an entry is also displayed called ***DefaultTemplate**. This entry is used when running Internet Server in the cloud and instances are started and stopped dynamically. The default template provides the default configuration for instances started dynamically.

SSH Server: SSH Server Status

As an administrator, you can start, stop, and display the status of the SSH server on Internet Server instances. The following table lists the function you can perform on this page.

Function	Operation
Start	Starts the SSH or SFTP service.
Stop	Stops the SSH or SFTP server service.
Server Status	Displays the status of the SSH or SFTP server service.

SSH Server: Configure SSH Server

As an administrator, you can configure the SSH or SFTP server for the Internet Server instances. When this page is entered, you must select the server that you want to configure. The following information can be configured for the SSH or SFTP server:

Parameter	Description
Enabled	Whether the SSH or SFTP server is enabled.
IP Port	Defines the ports that the SSH or SFTP service listens on for incoming SSH or SFTP server requests.
Bind Adapter IPV4 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
Bind Adapter IPV6 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
SSH System Key	Defines the system key used for incoming SSH requests.
Key or	Defines whether keys, certificates, or both are used for incoming requests

Parameter	Description
Certificate	that require key or certificate authentication.
Welcome Message	Defines the message displayed when an SFTP client log in is successful. Note that some SFTP clients do not display the SFTP welcome message.
SSH Algorithm Group	Overrides default SSH algorithms with SSH algorithms defined by the Add/Update SSH Algorithms page.

Note: In addition to the entries for each Internet Server, an entry is also displayed called ***DefaultTemplate**. This entry is used when running Internet Server in the cloud and instances are started and stopped dynamically. The default template provides the default configuration for instances started dynamically.

OFTP2 Server: OFTP2 Server Status

As an administrator, you can start, stop, and display the status of the OFTP2 server on Internet Server instances.

The following table lists the function you can perform on this page.

Function	Operation
Start	Starts the OFTP2 service.
Stop	Stops the OFTP2 server service.
Server Status	Displays the status of the OFTP2 server service.

OFTP2 Server: Configure OFTP2 Server

As an administrator, you can configure the OFTP2 server for the Internet Server instances. When this page is entered, you must select the server that you want to configure.

The following information can be configured for the OFTP2 server:

Function	Operation
Enabled	Defines whether the OFTP2 server is enabled.
IP Port	Defines the ports that the OFTP2 service listens on for incoming OFTP2 requests.
TLS Port	Defines the ports that the OFTP2 service listens on for incoming OFTP2 TLS requests.
Bind Adapter IPV4 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
Bind Adapter IPV6 Address	Defines whether Internet Server binds to an Adapter IP address when listening on a port.
OFTP2 System Key	Allows you to select an OFTP2 System key that is used for incoming OFTP2 TLS requests.

Note: In addition to the entries for each Internet Server, an entry is also displayed called ***DefaultTemplate**. This entry is used when running Internet Server in the cloud and instances are started and stopped dynamically. The default template provides the default configuration for instances started dynamically.

LDAP Sync

As an administrator, you can synchronize LDAP users with the MFT database. Users, and optionally rights, can be synchronized.

Review the Configuration: Authenticators page for information about configuring LDAP Authenticators.

The **LDAP Sync** page allows you to perform these functions:

- Sync one LDAP user.

- Sync one LDAP Authenticator.
- Sync all LDAP Authenticators.

Rights

The `AdministratorRight` is required to view and update the LDAP Sync.

Delegated Administration

Administration can be delegated only to super administrators.

Note: A super administrator is a user with **AdministratorRight** that is not assigned to a department.

Links

There are two links displayed for LDAP sync.

Task	Description
Sync User	Allows you to sync a single user. When this is selected, you must enter the User ID in the **Userid** field.
Sync All users in These Authenticators	All users in the selected authenticators will be synced. When you have entered the necessary information, click the **Sync** button. You should select an authenticator from the menu, or select `All`.

Note: Syncing an authenticator can take a few minutes, especially when you are syncing rights. A message is displayed at the top of the page with the status of the Sync request.

LDAP Sync works based on users in LDAP and the MFT database.

- If a user is in LDAP but is not in the MFT database, the user, and optionally, their rights, are added to the MFT database.
- If a user is in LDAP and is in the MFT database, the user, and optionally, their rights,

are synchronized to the MFT database.

- If a user is in the MFT database but is not in LDAP, the database user is disabled.

Lockout Management

As an administrator, you can view locked systems, users and IP addresses. A system, user or IP address is locked when the number of consecutive invalid log in attempts exceeds the defined thresholds in **Configuration > System Configuration > Lockout Rules**.

When this page is first entered, the **Results** table lists all of the locked users and IP addresses. The following table lists the buttons on this page:

Function	Operation
Release Selected Locks	Releases all selected entries.
Release All Locks	Releases all locks.
Release All User Locks	Releases all user locks.
Release All IP Address Locks	Releases all IP address locks.
Release All System Locks	Release all system locks.

When any of these buttons are selected, MFT communicates to all servers in the cluster to notify them that the selected locks must be released.

Note: MFT will not wait for a response. The release lock request is performed asynchronously and the admin page is not notified when a lock is released.

Activity

As an administrator, you can view and terminate active users for each MFT Internet Server and Command Center instance. It also allows you to view Internet Server Checkpoint records.

The following table lists the two links displayed for the **Activity** page:

Link	Description
Active users	Allows you to view and terminate active user sessions.
Internet Checkpoints	Allows you to view and terminate Checkpoint records.

Users

When this page is entered, the active users for the MFT instance you are logged into are displayed. An active user is a user that has successfully logged onto MFT, but has not logged off of MFT yet. You must select a host name to see the active users for that server.

To terminate an active user session, select the checkbox to the left of the user's line and click the **Delete** button.

Rights

The rights required for all active users are:

Right	Description
AdministratorRight	Allows you to list and terminate active user sessions.
ViewSessionRight	Allows you to list active user sessions.
UpdateSessionRight	Allows you list and terminate active user sessions.

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to a department cannot perform active user functions.

Internet Checkpoints

When this page is entered, all internet checkpoint records are displayed. Checkpoint records are created when Internet Server detects that an active transfer can be restarted. It saves the restart information in case the transfer terminates and needs to be restarted. Internet Checkpoints are typically deleted when a transfer completes. But if the transfer fails and a transfer restart is not attempted, internal checkpoint records may not be purged.

The **Search Criteria** filter allows you to filter the Internet Checkpoint records that are displayed. The **Results** table shows the Internet Checkpoint records that match the selection criteria.

To delete an internet checkpoint, select the checkbox to the left of the checkpoint's line and click the **Delete** button.

Rights

The rights required for all **Internet Checkpoint** pages are:

Right	Description
AdministratorRight	Allows you to list and delete internet checkpoints
ViewCheckpointRight	Allows you to list internet checkpoints
UpdateCheckpointRight	Allows you to list and delete internet checkpoints

Delegated Administration

Administration can be delegated to users in the following ways:

- Users with the required rights that are not assigned to a department.
- Users with the required rights that are assigned to a department cannot perform Internet Checkpoint functions.

Delegated Administration

Delegated administration offers an administrator the ability to divide the system into smaller units which can be managed independently of one another. This subdivision of the system offers greater security and eases the 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. The department administrator cannot administer anything else in the system. The existing system rights, such as UpdateTransferDefinitionRight, can also be applied to a department administrator thus offering a finer granularity of administrative control.

Administrators who are not assigned to a department are considered super administrators who can manage the entire system. While department administrators can only 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 system configurations, transfer server configuration, and checkpoints. They are also the only ones who can add departments and change the department to which a server is assigned.

Administrators can further limit the access to their users, groups, and servers through the use of visibility. Visibility supports departments to interact with each other without giving up administrative control. When applied to users, groups, and servers, visibility supports departments to expose or hide these items from each other. This is achieved by setting the **Visibility** parameter to public or private. For example, the Sales department can create a transfer and give authorization for that transfer to a user with public visibility 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 is with private visibility, the Sales department cannot give this user authorization to transfer the file. In this case the user is effectively hidden from other departments.

This design supports 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.

Administrative Functions and Rules

The department and visibility features affect how the administrative functions of TIBCO MFT Internet Server works when performed by department administrators and super administrators.

For the tasks that administrators can perform and what the task does when performed by department administrators and super administrators, see the following introductions:

- Active Users
- Audits
- Departments
- Diagnostics
- FTP Server Configuration
- Groups
- Server
- Server Credentials
- System Configuration
- Users

Active Users

Users with UpdateSessionRight can delete and view active users; while users with ViewSessionRight can only view active users.

Role	Description
Department Administrator	Department administrators with ViewSessionRight can only view active users in their departments.

Role	Description
	Department administrators with UpdateSessionRight can delete and view active users in their departments.
Super Administrator	Super administrators can view or delete any active users.

Audits

Audits records are assigned to the department from which the corresponding transfer definition is assigned. Audit records do not have visibility associated with them. An audit record can only belong to one department in the system. Department administrators can view audit records assigned to their departments and audit records assigned to the departments that they can manage.

Note: For more information of searching audits, see Search Audits. To perform audit searches, you must have ViewAuditRight.

Search Audits

Role	Description
Department Administrator	Department administrators can search for and display audit records that are assigned to their departments and to the departments that they can manage. When performing a search based on user ID, group ID, or server name, only those that are assigned to this department and to the department that the department administrator can manage can be used as search criteria. Department administrators can view audit records of file transfers assigned to their departments and audit records of file transfers assigned to the departments that they can manage, except in the case when a search is done based on a specific transfer user ID or a specific audit ID. Performing a

Role	Description
	search on a specific transfer user ID returns all audit records for that user no matter which department the transfer is assigned to. In the same way, performing a search on a specific audit ID returns the audit record for the transfer no matter which department the transfer is assigned to. This extended search capability is provided as a convenience for department administrators.
Super Administrator	Super administrators can search for and display all audit records in the system.

Delete Audits

Role	Description
Department Administrator	Department administrators cannot delete audit records.
Super Administrator	Super administrators can delete audit records older than a defined date, or older than a defined number of days.

Departments

The department administrative tasks can only be performed by a super administrator. Department administrators can only manage users assigned to their own departments and users assigned to the departments that they can manage.

Add Department

Role	Description
Department Administrator	Department administrators cannot perform this task.
Super Administrator	Super administrators can add departments to the system.

Manage Departments

Role	Description
Department Administrator	Department administrators cannot perform this task.
Super Administrator	Super administrators can list, update, and delete all departments in the system.

Diagnostics

Only super administrators can perform this task.

FTP Server Configuration

Only super administrators can perform these tasks.

Groups

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

Granting a group private visibility means that public users from all departments and private users from its own department can be added to it. This group ID can be managed by its own department administrator as well as by other department administrators that can manage the department assigned to this group. 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 is capable to do; and in addition, this group ID can be seen and is available to all department administrators in the system. This group can have public users from other departments added to it, and the group can be set as the authorized group ID in a file transfer definition that is assigned to other departments. The group can be used as the group ID value in a user profile definition created for public nodes assigned to other departments. Group IDs

must be unique throughout the system, thus groups in different departments cannot have the same group ID. A group can only belong to one department in the system.

Department administrators can see groups assigned to their departments, groups assigned to the departments that they can manage, and groups from other departments that have public visibility.

UpdateGroupRight supports users to add, update, delete, and view groups. ViewGroupRight supports users to view groups.

Add Group

Role	Description
Department Administrator	Department administrators can create a group, and assign the group to their departments or the departments that they can manage. The visibility of the group can be set to public or private.
Super Administrator	Super administrators can create a group which can be assigned to any department in the system or to none at all. The visibility of the group 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 super administrators.

Manage Groups

Role	Description
Department Administrator	Department administrators can update and delete any groups that are assigned to their departments and any groups that are assigned to the departments that they can manage. Department administrators can see and change the **Department** parameter of a group definition assigned to

Role	Description
	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 the department administrator.
Super Administrator	Super administrators can list, update, and delete any group in the system. The department that this group is 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. Pay special attention when changing the visibility of a group, because this change might include or exclude users.

Server

Servers can be assigned to departments and they can have a public or private visibility. Super administrators are the only ones who can perform the tasks of creating and configuring servers and assigning them to particular departments. Department administrators cannot add servers. Department administrators can list all servers assigned to their departments and 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 the server can be set as the server for a file transfer for a particular department. Servers can be associated with this server for public and private users or groups in this department.

Assigning public visibility to a server means that in addition to the features granted by private visibility, the server can also be set as the value of the **Server Name** parameter 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 supports users to update and view servers. ViewServerRight supports users to view a server.

Add Server

Role	Description
Department Administrator	Department administrators cannot perform this task.
Super Administrator	Super administrators can create a server which can be assigned 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

Role	Description
Department Administrator	Department administrators can update servers assigned to their departments and the departments that they can manage.
Super Administrator	Super administrators can update and delete all servers in the system. The department to which the server is assigned can be changed to any department in the system or to none.

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 are the only ones who can perform these tasks. Users and groups associated with server credentials can only be mapped to servers that are assigned to their departments or public servers in other departments. A private user or group in a

department can never be mapped to a server that is not assigned to that department of that user or group.

ViewServerCredentialRight supports users to view credentials.

Add Server Credentials

Role	Description
Department Administrator	Department administrators cannot perform this task unless specifically given UpdateServerCredentialRight.
Super Administrator	Super administrators can add 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

Role	Description
Department Administrator	Department administrators can list, update, and delete server credentials if they are given the proper rights. In addition to AdministratorRight, administrative users must also be given UpdateServerCredentialRight to perform this function.
Super Administrator	Super administrators can list, update, and delete any server credential definition in the system.

System Configuration

Only super administrators can perform these tasks.

Users

Users can be assigned to departments and they can have public or private visibility.

Granting a user private visibility means the user can be added to public and private groups that are assigned to the user's department, the user can be set as the authorized user of transfer definitions that are assigned to the user's department, and the user can have a server credential created for public and private servers assigned to the user's department.

Granting a user public visibility means the user can perform what a private user is capable to perform, can be added to a public group assigned to another department, can be set as the authorized user of a transfer definition that is assigned to another department, and 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 supports users to update users who have only TransferRight. ViewUserRight supports users to view users.

Add User

Role	Description
Department Administrator	Department administrators can create a user with TransferRight (default) and assign the user to their departments or any departments that they can manage. By default, the user is assigned to the departments to which the department administrators belong. Department administrators can assign users assigned to their departments or any departments that they can manage, the system administrative rights within these departments. This means department administrators cannot create super administrators, but they can create another administrator for their departments and any departments that they can manage. The visibility of the users can be set to **public** or **private**. Setting visibility to **public** makes the users visible and available for all 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.

Role	Description
	Super administrators can create super administrators, department administrators, and 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

Role	Description
Department Administrator	Using this feature, department administrators can create a new user and assign the user to their departments or any departments that they can manage. By default, the user is assigned to the departments to which the department administrators belong. The new user can be created from a pre-existing user from the departments to which the department administrators belong, or from a pre-existing user from the departments that the department administrators can manage. The new user is automatically given rights depending on the user that is being used as a template. However, department administrators cannot give the new user any rights that they do not have. For example, a department administrator who only has `UpdateServerCredentialRight` cannot assign `AdministratorRight` 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

Role	Description
Department Administrator	Department administrators can update users assigned to their departments and any departments that they can manage. Department administrators can change the department to which 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 department administrators.
Super Administrator	Super administrators can list, update, and delete all users in the system. The department that the user is 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 utilities.

Executing TIBCO MFT Internet Server File Transfer as a Postprocessing Action

Postprocessing 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 Command Line Utilities.

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

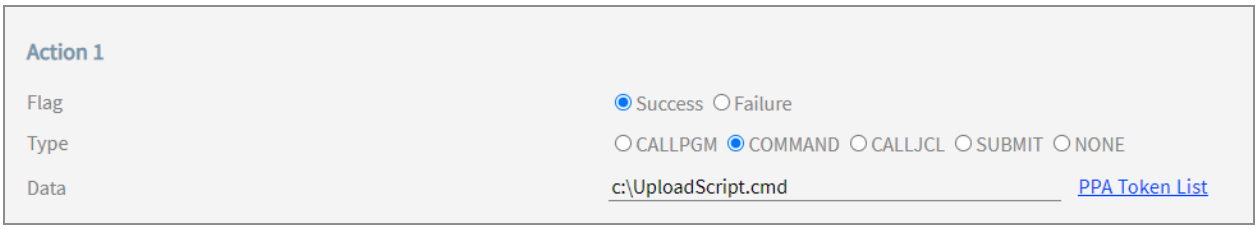
When using PPA to initiate an TIBCO MFT Internet Server Command Line Utility command or any command for that matter, it is good practice to get the command running successfully in batch mode first. For this example, first use the file transfer command for the Internet Server Command Line Client Utility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



After that, each time this transfer request is run, this PPA starts 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.

Note: 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:xercesImpl.jar:xmlParserAPIs.jar
# Execute the Java CFAdmin
java cfcc.CFAdmin t:$1.xml $2 $3 $4 $5 $6 $7 $8 $9
```

The above script performs the following functions:

- 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.

> **Note:** 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
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:

Property	Description
	• 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.

Before you begin

The `SIFTSingleFileTransfer` class is in `NonGUIApplet_0.0.0.1.jar` file which will be in the directory after installing the 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 on 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.

Parameter	Description
`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().
`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.

Parameter	Description
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 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, 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 .
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 , 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 on 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 on 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 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 **Configuration > 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 `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,

Parameter	Description
	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. **Note:** 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. **Note:** 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 are 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.

Note: 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/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 **Configuration > System Configuration** options or through the **Transfer** option.

   > **Note:** If the template is defined in both places, the Internet Server transfer definition overrides the 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.

> **Note:** 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 include 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 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 ensure 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

Line	Description
	receives an email, the data entered here will be shown as the Sender (or From). **Note:** 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

Line	Description
	directly to the screen where you can access the file. **Note:** 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.

Line	Description
	Note: 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

Token	Description
	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.

Note: 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 ensure 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.

Line	Description

`<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 , the data entered here will be shown as the Sender (or From).

`<recipient>`
`<address><token`
`name="recipientemailaddress"/></address>`
	This code is currently commented out. It defines the default recipient.
	
	If you define an email address in 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

Line	Description
	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

Token	Description
	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)*

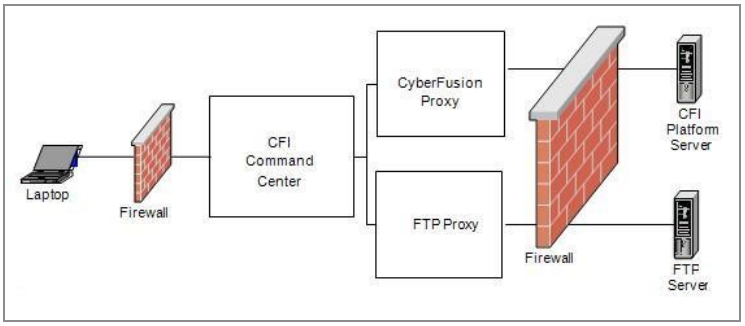
If tokens are available, you can click **File Token List** next to the **Server File Name** field on the Add Transfer page for the complete token list.

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 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.
`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

Parameter	Description
	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. **Note:** You need to configure this parameter when the FTP Proxy component is having trouble transferring through 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

Note: 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.

> **Note:** Files named `FA1240000001` and `FA1240000002` are examples of an error condition. They are shown here as an example of what the user may see when no `Virtual Alias` parameter is configured. They are the actual file IDs which 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.

> **Note:** Language preference is usually done automatically when working on an international version of Windows or can be controlled manually by setting the language preference in the browser.

- If the end user's preferred language is not one supported by 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 , 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.

Note: For installations using an MSSQL database that will be using Windows Authentication, you must add the domain parameter with the domain name to the end of the database URL. To do this, 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 provides nine JMS XML schema files ending with the `.xsd` extension and three accompanying sample XML files.

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

See the following introductions for details of the XML schema files or sample XML files:

- JMS XML Schema Files
- XML Files

JMS XML Schema Files

The JMS XML Schema files define the rules that must be followed when creating XML files and therefore should not be updated.

The JMS XML Schema files are located in the `<MFTIS_Install>/server/webapps/<context>/example/JMS` directory.

The following table lists the nine JMS XML Schema 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 searches 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

XML Schema File	Description
	and returns an array of 0 or more audit records. For the audit search, it returns a record for each transfer that matches the audit search filters. For other requests, it returns 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 • Internet Server Transfer Request • Platform Server Transfer Request
`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.
`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 . The following three request types are supported: • ManageConfigRequest: returns the JMS configuration parameters. • ManageServerRequest: returns a list of MFT servers defined to . • ManageServerTransfers: returns a list of

XML Schema File	Description
	predefined transfers. **Note:** The ManageServerRequest request returns 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. The following two types of responses 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

XML Schema File	Description
	request JMS type is ManageTransferRequestIS. This response returns all Internet Server transfers defined to that the user defined in the ManageRequest request is authorized to access.
`TransferRequestInternetServer.xsd`	Defines the format of the parameters required to initiate an Internet Server transfer. Internet Server transfers can only be initiated through JMS. Internet Server transfers can perform the following actions: • Read a JMS queue and send the data to a remote destination. • Read a local file and send the data to a remote destination. • Read data from a remote destination and write data to a JMS queue. • Read data from a remote destination and write data to a local file. Two JMS records can be returned for this request: • Immediate response: indicates whether the request is 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: this is written when a request is accepted and the

XML Schema File	Description
	`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 third-party transfer. TIBCO MFT Internet Server retrieves data from the JMS queue and initiates a transfer to Platform Server A to transfer a file to or from Platform Server B. Two JMS records can be returned for this request: • Immediate response: indicates whether the request is accepted and submitted to the Platform 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: this is written when a request is 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

The XML files define 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.

The following table lists the three sample 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.
`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.

Using JMS XML Files

Each sample XML file has a corresponding XSD file. TIBCO MFT Internet Server provides 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.

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 is only five digits in length for the initiator or responder platform transfers. All the other IDs 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

Byte	Description
	• 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 - Z: represent 2015 - 2036.
6 - 12	The sequential number in hex between 0 to FFFFFFF.

Appendix A: web.xml Parameters

Most TIBCO MFT Internet Server and TIBCO MFT Command Center parameters are configured through the Administrator web pages. But, some parameters, which are infrequently used or must be configured at server startup, must be configured in the `web.xml` file.

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 TIBCO Technical Support.

The `web.xml` parameters are defined by the context-param 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 changes of the `web.xml` file to take effect.

Note: If MFT detects an XML syntax error, the MFT server does not start. See the `catalina.out` file in the `<MFT_Install>\server\logs` directory for details.

The `web.xml` parameters are divided by functionality into the following categories:

- Security Parameters: parameters that affect the security of the MFT instance.
- Miscellaneous Parameters: parameters that do not fit into the other categories.
- Connectivity and Protocol Parameters: parameters associated with file transfers and file transfer protocols.
- OEM Parameters: parameters that can be used to change the product names and branding.
- Database Driver Parameters: parameters associated with the JDBC connection.
- Database Pooling Parameters: parameters associated with database pooling.

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 is not performed.	Defines the referrer URLs supported 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 separated by commas. **Note:** You should enter the URL for this MFT Server.
`AllowedReferersForXferNavigation`	By default, referrer URL checking is not performed.	Defines the referrer URLs supported 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. **Note:** You should enter the URL for this MFT Server.
`AllowUserDefinedJavaClasses`	True	Defines whether admins can configure **Alert Action> Execute Java Class** and **Scheduler definition>Scheduler Job Type> Execute Java Class**.

Parameter	Default	Description
		Valid values are: **true**: Allows admins to configure and execute user defined java classes **false**: Does not allow admins to configure or execute user defined java classes
`Anonymous`	No default	Defines users that can log in without password validation. Make sure that these users have limited file transfer authorization. More importantly, make sure that these users do not have any administrator rights.
`BCFipsMode`	False	Defines whether MFT uses 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. **Warning:** 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 TIBCO Technical Support to change this.

Parameter	Default	Description
`ChangedPasswordEmailEnabled`	No	Defines whether an email is to be 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 "SAN:OtherName:PrincipalName" as the user ID.
`InstallAdminService`	Set during installation	Defines whether the Administrator service is installed on an Internet Server instance.

Parameter	Default	Description
		If the Administrator service is installed, this parameter is set to YES. If you set it to NO, Administrator service requests for this Internet Server fail. **Note:** If the Administrator service for the Internet Server instance is not installed and is set to NO by the installer, setting this parameter to YES is ignored.
`LoadBalancerIPAddressList`	No default	Applies to HTTP and SFTP file transfer requests. For HTTP requests that go through a load balancer, MFT uses 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. For SFTP transfers, MFT can extract the originating IP address 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 semicolon. Specifying *All accepts the **HTTP X-Forwarded-For** header from any incoming IP Address. This can be used when the load balancer IP

Parameter	Default	Description
		address is not static.
`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 does not contain a privacy policy link. When any value is defined, the **View Privacy Policy** link is displayed on the footer of each page. You can click this link to open a privacy policy page. **Note:** MFT does not provide a privacy policy page. You must define a privacy policy page that is 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 defined timeout, the next request fails. The HTTP timeout is set by the

Parameter	Default	Description
		`SessionTimeOut` parameter configured in the `web.xml` file located in the *<MFT_Install>*`\server\conf` directory.
`SmtpTLSEnabled`	false	Defines whether SSL/TLS is used when communicating to an SMTP server. The value of false indicates that SSL/TLS are not used. The value of true indicates that the SMTP communication is performed using SSL.
`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. **Note:** This setting is quite strict and many clients might stop working at the Strong or Paranoid level.

Parameter	Default	Description
`SSOAllowRest`	true	User can login using REST calls when this parameter is set to `true` and `SSOLoginRequired` is also set to `true`.
`SSOLoginRequired`	false	When this parameter value is set to `true`, the user is required to log in through SSO rather than the user ID and password.
`SSOExcludedUsers`	No default	Defines the list of user IDs that do not require OIDC. Each user ID is separated by a comma.
`UnsecuredHTTPSupport`	NO	Defines whether HTTP requests are accepted. The default value of NO indicates that HTTP requests are not accepted. When it is set to YES, HTTP requests are accepted if an HTTP connector is defined.

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

Parameter	Default	Description
		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.
AzureClientConfigFile	No default	Defines the Azure config file name. Do not change this parameter unless instructed to do so by MFT Technical Support.
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

Parameter	Default	Description
		Internet Server and Command Center checks for cache updates. It also defines how frequently Internet Server and Command Center checks 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_

Parameter	Default	Description
		TEMPLATENAME environment variable. **Note:** Only Command Centers or Internet Servers with the administrator service installed can check for inactive servers.
`DefaultTransferClient`	browser	Defines the default transfer client. The value, namely browser, indicates the default transfer client is the browser client. It is good practice to use the browser client by default. The value of java indicates 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.
`HostName`	The host name defined during installation	Defines the host name that is set during the configuration process.

Parameter	Default	Description
		This parameter is used to identify the MFT server in the database tables. This should not be changed without guidance from TIBCO 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	This parameter is 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 must 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.
`MaxCollectionRecordCnt`	500	Defines the number of

Parameter	Default	Description
		records that can be collected from a Platform Server on a collection request. Valid value for this parameter is a numeric value between 50 and 500.
`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 lower 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.

Parameter	Default	Description
		Note: 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 you to update the `SAMLAuthenClassRef` used in the SAML negotiation. **Note:** Only do this if you are using a non-standard `SAMLAuthenticationClassRef` and are instructed by MFT Support to change this field.
`SAMLComparison`	MINIMUM	Allows you to update the SAML Comparison method. The default value of MINIMUM is suggested. Other supported values are: EXACT, MAXIMUM or BETTER. **Note:** Only change this field if you are instructed to do so by MFT Support.
`SAMLNameIDType`	urn:oasis:names:tc:SAML:2.0:na	Allows you to update

Parameter	Default	Description
	meid-format:transient	the `SAMLNameIDType` used in the SAML negotiation. **Note:** Only do this if you are using a non-standard SAML name ID type and are instructed by MFT Support to change this field.
`SharePointTempDirectory`	<MFT-Install>/server/webapps/cfcc/WEB-INF/sharepoint	Allows you to override the directory where temporary encrypted sharepoint files are written.
`SSHDKeepAliveInterval`	30 seconds	Defines the interval between SSH KeepAlive requests for the MFT SSH Server.
`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

Parameter	Default	Description
		indicates that MFT does not perform an audit search when the Search Audits page is first configured. Searches are on demand when the user defines the selection criteria and click **Search**.
`SendGlobalEmail`	true	This parameter is not used.
`SendMFTTrustedCerts`	false	Valid values are: • 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 defines the SOAP calls

Parameter	Default	Description
		to be compatible with older versions of MFT. Any RETRIEVE or GET call returns data in the format defined by MFT version 7.2.4.
StatisticsUpdateInterval	10	MFT asynchronously updates the DB MFTStatistics table to improve performance. This parameter defines the frequency of statistics updates in seconds. If no transfers have completed in this interval, MFT will bypass the statistics update for this interval.
StoreAndForwardTempDir	<MFT-Install>/server/webapps/cfcc/WEB-INF/tempstore	Defines the directory where Internet Server writes temporary data when performing virus checking or DLP scanning in a Store and Forward mode. You must define the fully qualified directory name.
SyncLdapAtLogon	true	Defines whether an LDAP user are synchronized with the LDAP authenticator when HTTP users log

Parameter	Default	Description
		on. The value of True indicates that LDAP users are synchronized when the user logs on. The value of False indicates that LDAP users is not synchronized with the LDAP authenticator when the user logs on. The synchronization is performed when the on-demand or scheduled synchronization occurs.
`TraceDir`	The directory defined during installation	Defines the directory where MFT trace files are located.
`TransferJMSThreadPoolSize`	100	Defines the number of threads that are used to execute JMS Internet Server or Platform Server transfer requests. This parameter limit the number of concurrent JMS initiated transfers to the defined value.
`ValidationQueryTimeout`	1	Defines the number of seconds that MFT waits for a DB Pooling

Parameter	Default	Description
		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. **Note:** Do not change this parameter unless instructed to do so by MFT Technical Support.
`reuseJMSConnection`	false	Valid values are: • True: Reuses JMS connections. • False: Creates a new JMS connection for each request.

Parameter	Default	Description
		Note: This parameter should be used for EMS only.
`tilesDefinitions`	/WEB-INF/tiles.xml	This parameter must not be changed.

Connectivity and 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 Command Center Admin API REST calls.
`admin-service-enabled`	True	Enables Admin API REST calls.
`ft-service-enabled`	True	Enables file transfer API calls.
`AllowCustomServerDefinition`	True	Stops admins from adding Custom server definitions and also disable all transfers going to a Custom server. Valid values are: **true**: Allows custom

Parameter	Default	Description
		server definitions. **false**: Does not allow custom server definitions.
`AllowLocalServerDefinition`	True	Stops admins from adding LOCAL server definitions and also disable all transfers going to a local server. Valid values are: **true**: Allows local server definitions **false:** Does not allow local server definitions
`AllowEmailServerDefinition`	True	Stops admins from adding Email server definitions and also disable all transfers going to an Email server. Valid values are: **True**: Allows Email server definitions. **False**: Does not allow Email server definitions. **Defined**: Allows Email server

Parameter	Default	Description
		definitions but only allows Email transfers to defined users.
`AllowMailboxServerDefinition`	True	Stops admins from adding mailbox server definitions and also disables all transfers going to a mailbox server. The valid values are: **True**: Allows mailbox server definitions. **False**: Does not allow mailbox server definitions. **Defined**: Allows mailbox server definitions but only allows mailbox transfers to defined users.
`AS2Acknowledgement`	No default	When very large AS2 requests are received or sent, set this parameter to deferred. Encrypted AS2 data is written to the directory defined by the `AS2TempDirectory` parameter and then

Parameter	Default	Description
		processed.
`AS2FollowRedirects`	Yes	Defines whether to follow http redirect (302) when connecting to a partner AS2 server. Valid values are: `Yes`: Follow redirects `No`: Do not follow redirects **Note:** Set this value to `No` only when redirects seem like a security vulnerability.
`AS2TempDirectory`	No default	Defines the AS2 temporary directory. This parameter is generally defined only when very large (larger than 500MB) AS2 files are transferred. This parameter defines MFT to use a two-stage AS2 transfers. For uploads to MFT, encrypted AS2 data is written to this

Parameter	Default	Description
		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 it to a disk.
`ChannelLimitSSH`	10	Defines the number of SSH channels per connection. **Note:** Versions prior to 8.5.0 incorrectly set this value to 800.
`DenyLoginIds`		Allows you to define one or more comma delimited users that cannot log in to the Internet Server or the Command Center. For example, you can add "root, administrator, support" so that

Parameter	Default	Description
		authentication by these users are not be attempted.
`DisplayFTPBanner`	YES	Defines whether the FTP/SFTP banner is displayed when the user logs on. Valid values are: 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	Defines 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

Parameter	Default	Description
		instance. If defined, this parameter overrides the Systems Configuration: Global FTP Settings "Number of Ports to Use" parameter value. **Note:** 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: FTP Settings "Starting Port" parameter value. **Note:** This parameter is ignored for Command Center.
`MaxConnectionCnt`	800 connections	Defines how many TCP connections are processed by each

Parameter	Default	Description
		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. **Note:** This parameter is deprecated and is replaced by `MaxConnectionCntFTP`, `MaxConnectionCntSSH`, and `MaxConnectionCntCF` parameters.
`MaxConnectionCntFTP`		Defines how many TCP connections are processed by the MFT FTP/FTPS Server. This parameter replaces the MaxConnectionCnt

Parameter	Default	Description
		parameter for FTP/FTPS connections.
MaxConnectionCntSSH		Defines how many TCP connections are processed by the MFT SSH/SFTP Server. This parameter replaces the MaxConnectionCnt parameter for SSH/SFTP connections.
MaxConnectionCntCF		Defines how many TCP connections are processed by the MFT Platform Server. This parameter replaces the MaxConnectionCnt parameter for Platform Server connections.
MaxConnectionCntOFTP2		Defines how many TCP connections are processed by the MFT OFTP2 Server.
OFTP2CfgFile	oftp2cfg.properties	Defines the infrequently used OFTP2 parameters in the server definition OFTP2 options tab.

Parameter	Default	Description
		There are many additional OFTP2 configuration parameters that are not defined in this tab. The web.xml parameter `OFTP2CfgFile` points to the OFTP2 config file that defines these additional parameters. The default file "`oftp2cfg.properties`" is located in the WEB-INF directory. **Important:** You must only update this file when instructed to by TIBCO Technical Support.
`ReCaptchaExcludedUsersList`	None	Defines users that do not need to be verified by ReCaptcha. This parameter was added in case there was a problem with ReCaptcha and it needs to be disabled. You can add multiple users by delimiting the users with a

Parameter	Default	Description
		comma. When these users logon, ReCaptcha is still displayed on the login page, but MFT does not perform ReCaptcha verification. This parameter only applies to the log in page.
`ReCaptchaVerificationUrl`	https://www.google.com/recaptcha/api/siteverify	Defines the Google ReCaptcha verification URL. Do not change this value unless the Google ReCaptcha verification URL changes.
`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

Parameter	Default	Description
		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	Defines 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 insecure diffie-hellman-group1-sha1 algorithm	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

Parameter	Default	Description
		`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.
`StoreAndForwardTempDir`	WEB-INF/tempstore	Defines the temporary files created during Storage and Forward AV and DLP checking are stored in this directory. These files are encrypted using a unique AES256 encryption key and are deleted when the transfer ends.
`TCPBufSize`	1024000	Defines the TCP buffer size used by SSH, FTP, and Platform Server connections.

Parameter	Default	Description
		Using a high value increases performance over connections with high latency.
`TLSCipherSuite`	None	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 typically defaults to using secure cipher suites during installation. **Note:** HTTPS cipher suites are defined in the HTTPS connector in the `server.xml` file located in the`<MFT_Install>/server/conf` directory.
`TLSProtocols`	TLSV1, TLSV1_1, TLSV1_2	Defines the protocols supported by FTP and Platform Server SSL connections.

Parameter	Default	Description
`TLSSecurityProvider`	The default MFT security provider	Defines the security provider used by FTP and Platform Server SSL connections.
`TransferThreadCntSSH`	10	Defines the number of SSH threads to process transfers. For a high volume of SSH transfers, you can set this parameter to the number of the CPU cores on the machine. This parameter is used by Internet Server and is ignored by Command Center.
`TurnOnLocalPPATrace`	false	Enables local PPA trace even if the tracing is `OFF`. Valid values are: `true`: Traces all Internet Server PPA execution. `false`: Does not trace Internet Server PPA execution.
`UserSessionLimit`	None	Defines the number of concurrent sessions that a user

Parameter	Default	Description
		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.
`ThrowEnvKeyPwdException`	True	If set to true this parameter prevents prompting of an exception when MFT fails to decrypt a password. MFT cannot decrypt a password if the `COM_TIBCO_MFT_ENCRYPT_KEY` environment variable is not set, or if the environment variable is set incorrectly. The following values

Parameter	Default	Description
		are valid for this parameter: • `true` • `false`

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 to be displayed when the product name of TIBCO MFT Command Center is displayed.
`OEM-CompanyName`	Cloud Software Group, Inc.	Defines the text to be displayed when the long company name is displayed on a web page.

Parameter	Default	Description
`OEM-CompanyURL`	http://www.tibco.com	Defines the URL of the link to the TIBCO website.
`OEM-Copyright`	Copyright (c) 2003-2016. Cloud Software Group, 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 to be displayed when the short product name of TIBCO MFT Internet Server is displayed.
`OEM-InternetServerName`	Internet Server	Defines the text to be displayed when the product name of

Parameter	Default	Description
		TIBCO MFT Internet Server is displayed.
`OEM-LongProductName`	TIBCO Managed File Transfer	Defines the text to be displayed when the long product name is displayed on a web page.
`OEM-PlatformName`	Platform	Defines the text to be displayed when the short product name of TIBCO MFT Platform Server is displayed.
`OEM-PlatformServerName`	Platform Server	Defines the text to be displayed when the product name of TIBCO MFT Platform Server is displayed.

Parameter	Default	Description
OEM-ProductURL	http://www.tibco.com/products/automation/application-integration/managed-file-transfer/default.jsp	Defines the URL of the link to the TIBCO website for the MFT server.
OEM-ShortCompanyName	TIBCO	Defines the text to be displayed when the short company name is displayed on a web page.
OEM-ShortProductName	MFT	Defines the text to be 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
DBType	No default	Defines the database type.

Parameter	Default	Description
		This value should not be changed unless directed to by TIBCO MFT Support.
DBConn	The JDBC URL defined during installation	Defines the JDBC URL. This parameter is rarely changed after the MFT installation. It can occasionally be changed when you want to add the SSL support or the High Availability support.
DBDriver	The JDBC driver class name defined during installation	Defines the JDBC driver class. This parameter is rarely changed 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. When the COM_TIBCO_MFT_CE_DB_PWD environment variable is defined, it overrides the **DBPass** and **DBPWDEncrypted** web.xml parameters.
DBUser	The database user defined during installation	Defines the database user associated with the JDBC connection.

Parameter	Default	Description
`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.

Parameter	Default	Description
`MaxIdle`	20	Defines the maximum number of idle connections that should 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 for a connection to be idle before it is eligible for eviction.
`MinIdle`	10	Defines the minimum number of idle connections that should be kept in the database pool at all times.
`TestOnBorrow`	true	Defines whether existing connections in the pool should be tested before use. It is good practice to set this parameter to true.
`TestOnReturn`	false	Defies whether existing connections in the pool should 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 wait 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 second	Defines 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

Parameter	Default	Description
		server/conf directory. org.apache. `tomcat.jdbc.pool.level = ALL` It should show up in the console or in the `catalina.log` file

Appendix B: Connection Manager

Connection Manager solves a common problem typically found when a server in the DMZ needs to communicate with a server in the internal network.

For example, TIBCO MFT Internet Server generally executes in the DMZ to support external client access; Internet Server must connect to the following servers executing in the internal network, and therefore must make TCP connections with these servers.

- LDAP Server for Authentication
- Oracle Server DB Instance
- TIBCO MFT Platform Server where data resides

Many firewalls are configured to not support TCP connections to be opened from the DMZ to the internal network. When supported, a security exception is often required. With Connection Manager, DMZ server instances can create connections to servers in the internal network without opening the connection from the DMZ; all connections are opened from the internal network.

Connection Manager Components

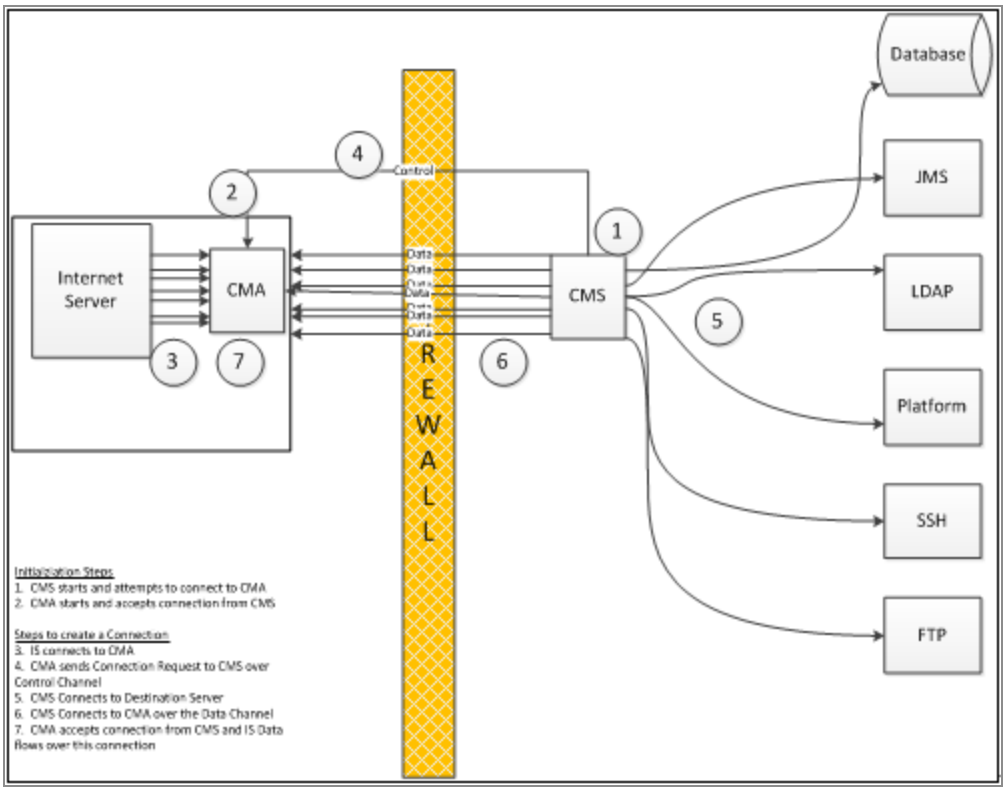
Connection Manager provides the following components: Connection Manager Agent (CMA), Connection Manager Server (CMS), , and TIBCO MFT Internet Server.

For more information on connection manager components, see *Appendix I: Connection Manager in the Installation Guide*.

Connection Manager Data Flow

Connection Manager can work in a simple environment or two-tiered DMZ structure.

The following figure shows a simple Connection Manager data flow:



The following brief explanation shows how Connection Manager works.

Initialization Steps:

1. When CMS is started, it attempts to make a connection to each CMA. If the connection cannot be established, CMS waits 30 seconds and tries again. It continues retrying the connection until the connection is successfully established.
2. At some point, CMA is started and listens for incoming CMS connections. CMA listens for TCP connections on the following two ports:
    - 48000: control connection from CMS
    - 48001: data connections from CMS

    When CMS retries the connection to the CMA control port, the connection is established successfully.

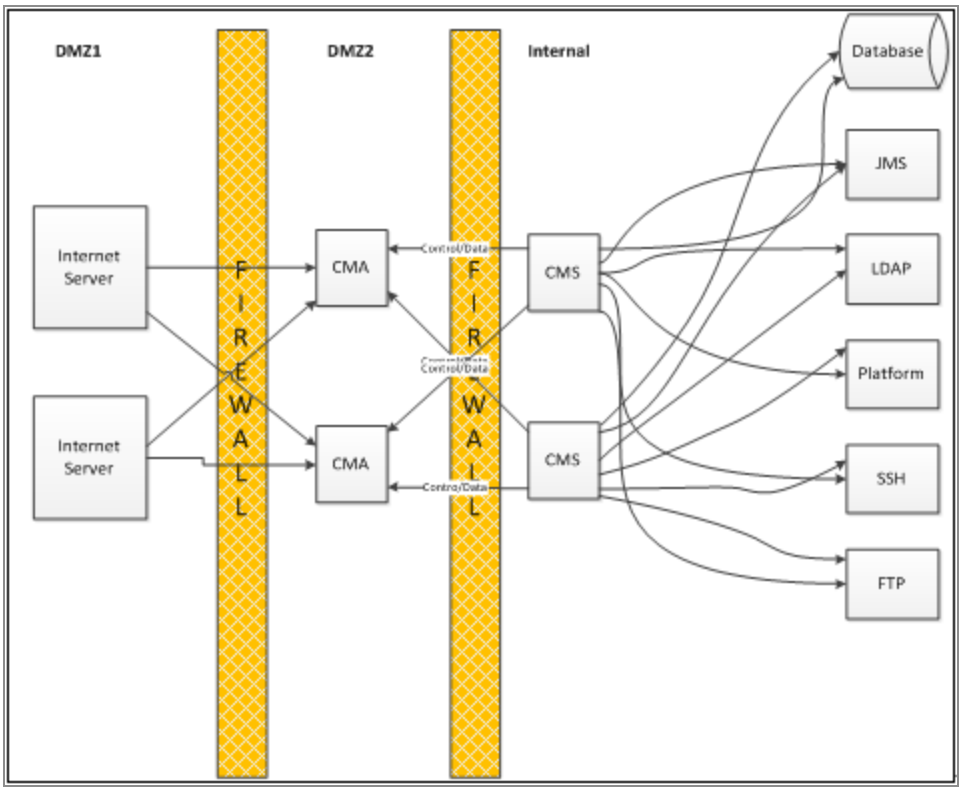
Steps to Create a Connection:

1. When an Internet Server needs to establish a TCP connection, it must first determine whether the connection must be routed through Connection Manager. Internet Server reviews its configuration to find a match on an IP address or IP address subnet.

Assuming that the connection must be made through Connection Manager, Internet Server requests a TCP connection with CMA. It then sends a SOCKS packet to CMA indicating the destination connectivity information (IP address and IP port).

2. CMA reads the Internet Server data packet and sends the request to CMS over the control connection.
3. CMS reads the data from the control connection and establishes a connection with the destination server.
4. CMS then establishes a TCP connection with the CMA data port. CMA ties this connection together with the connection request from Internet Server.
5. CMA accepts the connection from CMS and the Internet Server data begins to flow over this connection.

The following figure shows a two-tier DMZ architecture:



In this two-tier architecture, Internet Server is executing in DMZ1, while CMA is executing in DMZ2.

This architecture also shows the high availability capability of Connection Manager. Internet Server can connect to multiple CMA instances and CMA can accept requests from

multiple CMS instances. Internet Server connects to the first CMA instance that is available and CMA requests a connection on the first active connection to a CMS instance.

Performance Implications of Using Connection Manager

Connection Manager replaces the single connection between Internet Server and the target server (for example, Oracle DB) with three connections (Internet Server-CMA, CMA-CMS, and CMS-Oracle). Therefore, TCP connection establishment takes longer when using Connection Manager as compared to direct connections initiated by Internet Server.

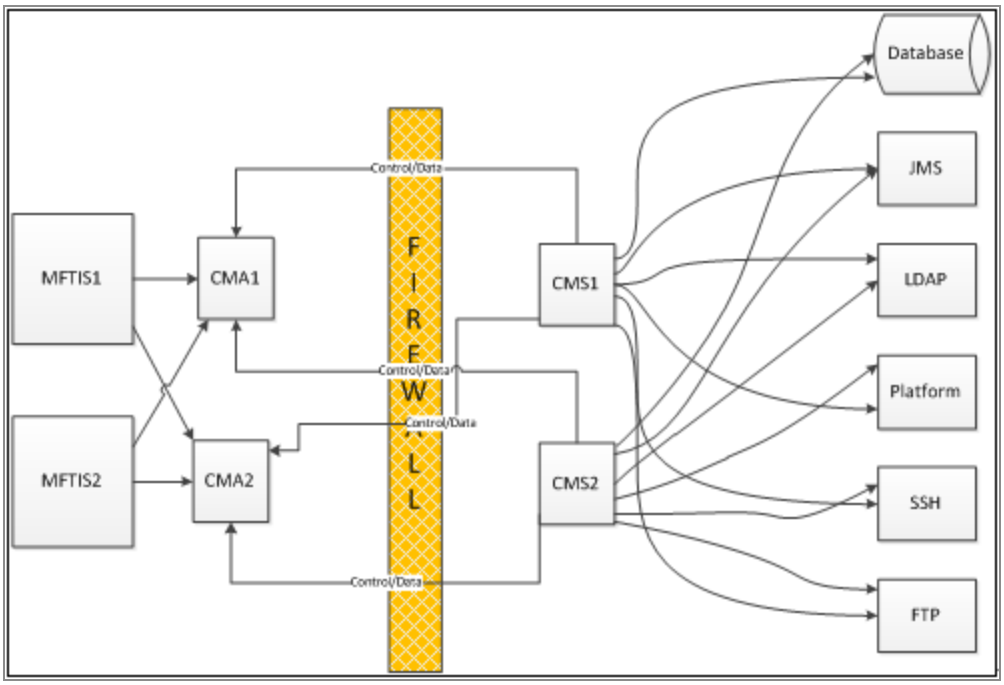
When connecting to internal servers that require many connections (for example, Internet Server connections to Oracle DB), it is best practice to minimize the number of connections established. Use of MFT Connection Pooling can minimize the number of TCP connections created between Internet Server and the Oracle DB server.

Slight performance degradation also exists when Internet Server uses Connection Manager to send bulk to internal servers. For example, Internet Server often needs to send gigabytes of data to TIBCO MFT Platform Server in the internal network. Instead of sending the data over a single connection, the data needs to be sent over multiple connections (Internet Server-CMA, CMA-CMS, and CMS-Platform Server). Many variables can affect the performance of file transfers using Connection Manager: Client network bandwidth, file size, and latency. At best, negligible performance differences exist between direct connections. Initial tests show approximately 10% - 15% performance degradation when used in a high volume, low latency, and fast network. After connections are made, CMA and CMS just pipes data from the source connection to the target connection and therefore use very little CPU and very little memory. To save CPU cycles, data is piped to the remote destination exactly as sent or received by Internet Server. If you want to encrypt the data, you must configure the Internet Server to use secure protocols.

Connection Manager High Availability

Connection Manager supports high availability.

The following figure shows how high availability can be configured:



To configure high availability, you must conform to the following rules:

- Create two or more CMS instances in the internal network, executing on different computers.
- Create two or more CMA instances in the DMZ, executing on different computers.
- Create two or more Internet Server instances in the DMZ, executing on different computers.

> **Note:** CMA and Internet Server can execute on the same computer or on different computers.

- CMS1 and CMS2 must be configured to connect to CMA1 and CMA2.
- CMA1 and CMA2 must be configured to accept connections from CMS1 and CMS2.
- CMA1 and CMA2 must be configured to accept connection requests from MFTIS1 and MFTIS2.
- MFTIS1 and MFTIS2 must be configured to connect to CMA1 and CMA2.

Connection Manager operates in an active or passive mode. Requests are sent to the first available component. If the connection to that component fails or is not available, the Connection Manager attempts to send the request to the next component.

The configuration in the figure above works as follows.

Note: MFTIS1 needs to connect to a Platform Server in the internal network.

1. At startup, CMS1 and CMS2 both attempt to establish connections to CMA1 and CMA2. If any connection requests fail, CMS1 and CMS2 continue to connect to CMA every 30 seconds until the connection request is successful.
2. MFTIS1 attempts to connect to CMA1 to perform this connection. Assume that CMA1 is not available; MFTIS1 then connects to CMA2.
3. CMA2 looks for an active control connection from CMS. If CMA has an active control connection with CMS1, it initiates the request to CMS1. Assume no active control connection to CMS1 is available; CMA2 then initiates the request to CMS2 over an active control connection.
4. After CMA2 makes an active connection to CMS2, CMS2 connects to the target Platform Server.
5. CMS2 then connects back to CMA2 over the data connection port (48001).
6. CMA2 then completes the connection with MFTIS1. Data begins to flow over the connection: MFTIS1 > CMA2 > CMS2 > Platform Server.
7. CMA2 issues heartbeat requests to CMS2 every 45 seconds. If no response is received within 30 seconds, CMA2 breaks the connection and waits for CMS2 to initiate a new connection.
8. CMS2 waits for heartbeat requests from CMA2. If no heartbeat request is received within 90 seconds, CMS2 closes the connection to CMA2 and attempts to re-establish the connection to CMA2. If this fails, the CMS2 attempts to connect to CMA2 every 30 seconds.

Configuring High Availability Using the Administrator Pages

During the installation process, Connection Manager is installed without the high availability capacity. You can use the Administrator pages to configure Connection Manager for high availability through the **Management > Connection Manager Nodes** option.

To create a high availability environment, you must make the following configurations:

- Install multiple CMA and CMS Instances.
- Configure each Internet Server to connect to multiple CMA instances.

  When configuring Internet Server, configure multiple CMA hosts and ports by separating the entries with a semicolon. For more details, see Updating Internet Server Configuration Information.
- Configure each CMS to connect to multiple CMA instances.

  When configuring CMS, configure multiple CMA IP addresses and host names. For more details, see Updating CMS Configuration Information.
- Configure CMA to accept connections from multiple Internet Server and CMS instances. For more details, see Updating CMA Configuration Information.

Connection Manager Load Balancing

Because most Internet Server instances are located on the same computer as CMA, Internet Server connects to the first available CMA. If the first CMA is not available, it connects to the next defined CMA.

When CMA needs to request a connection from CMS, CMA randomly requests the connection from one of the control connections already established by the CMS servers. If that request fails, CMA requests the connection from another CMS control connection.

CMA and CMS servers do not use substantial amounts of CPU or memory, so load balancing is not generally beneficial.

Configuring Connection Manager

When the Connection Manager components (CMA, CMS, and Internet Server) are installed, default values are set which can support Connection Manager to work in most installations. supports you to update the configurations of the components in the Administrator pages.

The Connection Manager configuration pages can be accessed through the following options:

- **Management > Connection Manager Nodes > Add Connection Manager Node**

- **Management > Connection Manager Nodes > Manage Connection Manager Nodes**

> **Note:** If you want to use to configure CMA, CMS, and Internet Server, firewall ports must be opened to allow to communicate with CMA, CMS, and Internet Server. For more information on the required ports and firewall settings, see Connection Manager Ports and Firewall Considerations.

The help pages for the Connection Manager Administrator pages describe in great detail the parameters on the individual pages. See the help pages for detailed information on the parameters.

In addition to updating the component configurations through the Administrator pages, you can configure the Connection Manager parameters through configuration files. CMS, CMA, and Internet Server Connection Manager configuration parameters are saved in .xml files. You can use a text editor to configure the Connection Manager parameters. Use a text editor to configure the CMA, CMS, and Internet Server configuration files only when you cannot use them to configure these files.

You can find the configuration files in the following directories:

- MFTIS: `<MFTIS Install>/server/webapps/cfcc/WEB-INF/reverseProxyDmz.xml`
- CMA: `<CMA Install>/webapps/connmgr/WEB-INF/reverseProxyDmz.xml`
- CMS: `<CMS Install>/webapps/connmgr/WEB-INF/reverseProxyInternal.xml`

For more information on the configuration files, see Connection Manager Configuration Files.

Adding Connection Manager Components

Before configuring the Connection Manager components, each component must be defined to . This is done through the Add Connection Manager Node page.

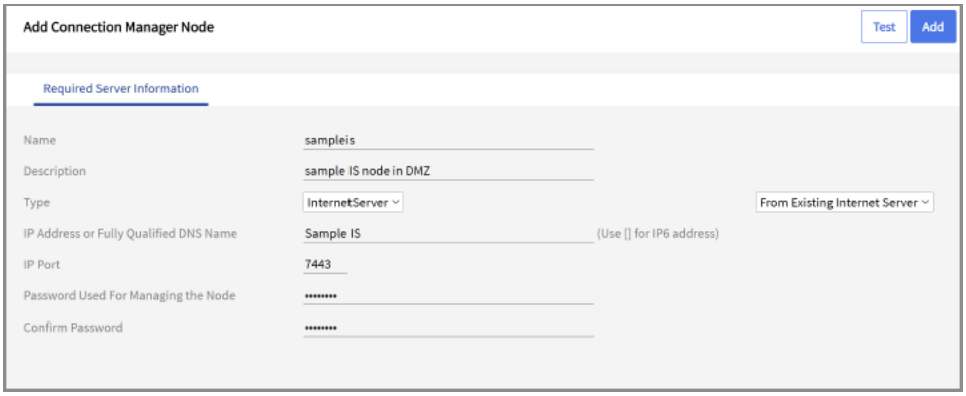
On this page, you can define the connectivity information required to communicate with the Connection Manager component.

The following figure shows the Add Connection Manager Node page. The **Type** parameter defines the Connection Manager type (CMA, CMS, or Internet Server). As you change the type, the **IP Port** field changes to the default value for that node type.

Note: The value of the **Password Used for Managing the Node** field must match the password entered when the component is first installed.

On this page, you can click the **Test** button to verify that the IP address, IP port, and passwords are defined correctly. When the test is successful, click **Add** to add the component.

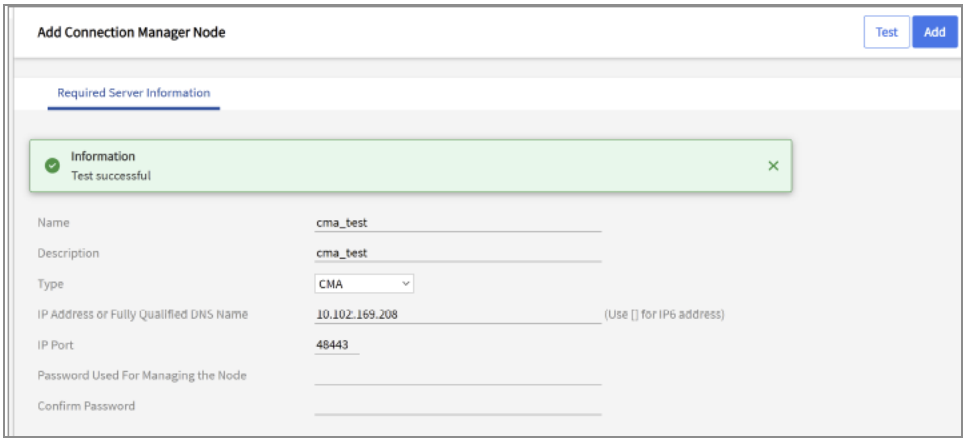
Add Connection Manager Node: Internet Server



When the **Type** parameter is set to `InternetServer`, you can use the **From Existing Internet Server** drop-down box to extract the IP address and IP port from an Internet Server that is installed.

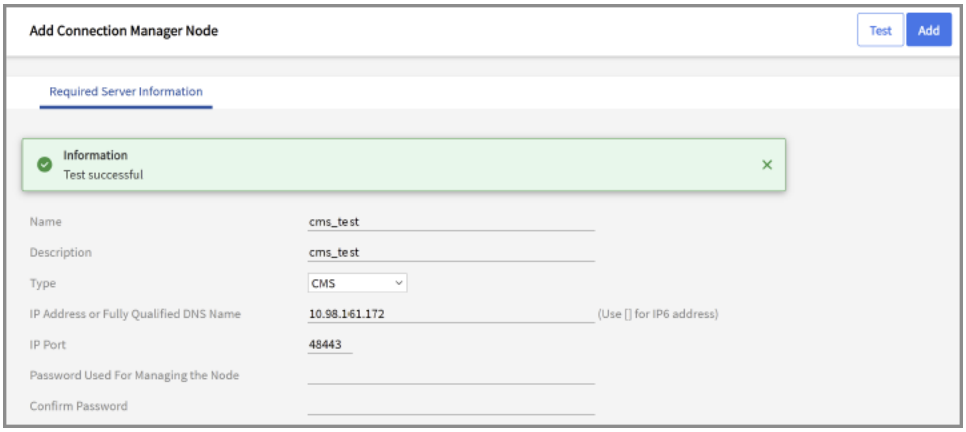
Click **Test** before adding the node to ensure that the type, IP address, IP port, and passwords are configured correctly.

Add Connection Manager Node: CMA



Click **Test** before adding the node to ensure that the type, IP address, IP port, and passwords are configured correctly.

Add Connection Manager Node: CMS

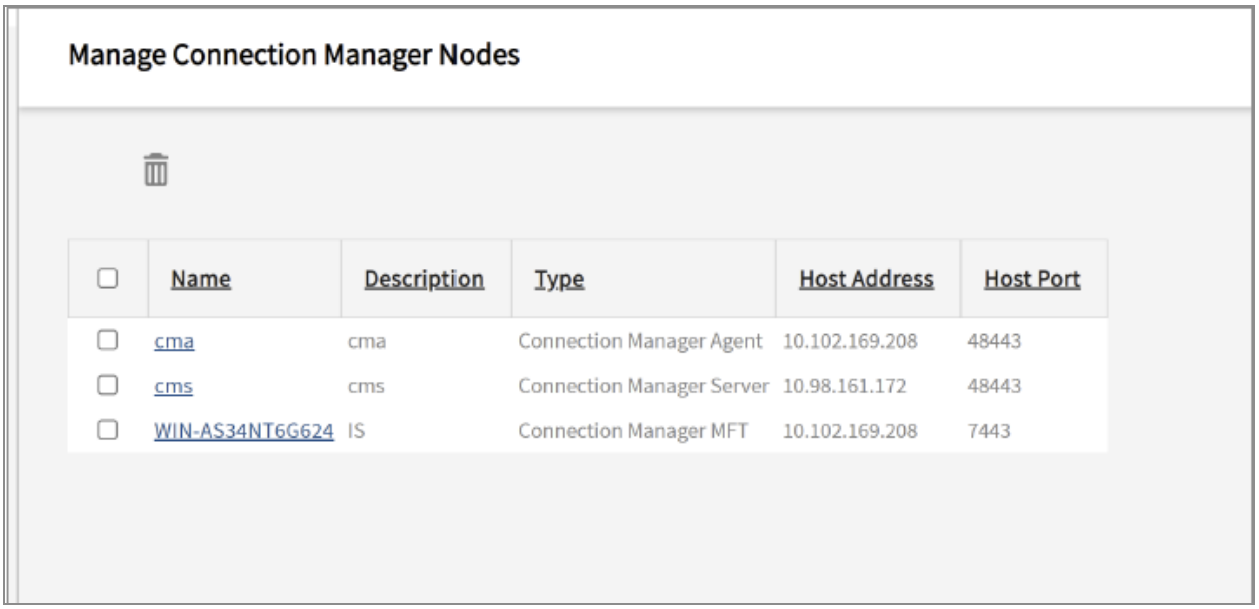


Click **Test** before adding the node to ensure that the type, IP address, IP port, and passwords are configured correctly.

Managing Connection Manager Nodes

You can use the **Manage Connection Manager Nodes** page to view and update the Connection Manager nodes defined.

The following figure shows the **Manage Connection Manager Nodes** page:

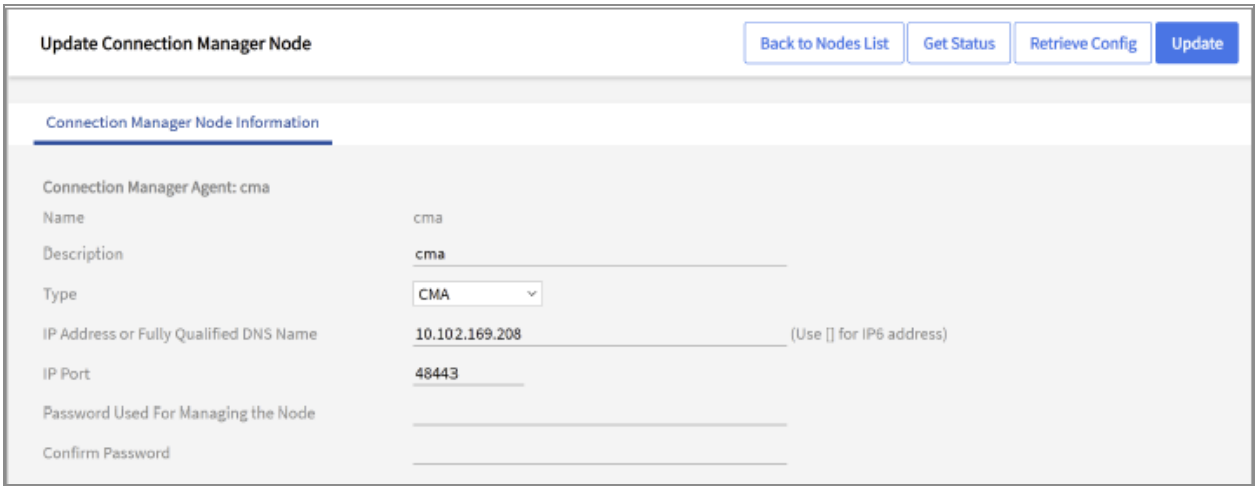


You can click an entry in the Name column in the **Results** table to get the detailed information for this node and update this node.

To delete Connection Manager nodes, select one or more checkboxes under the **Delete** column and then, click **Delete**.

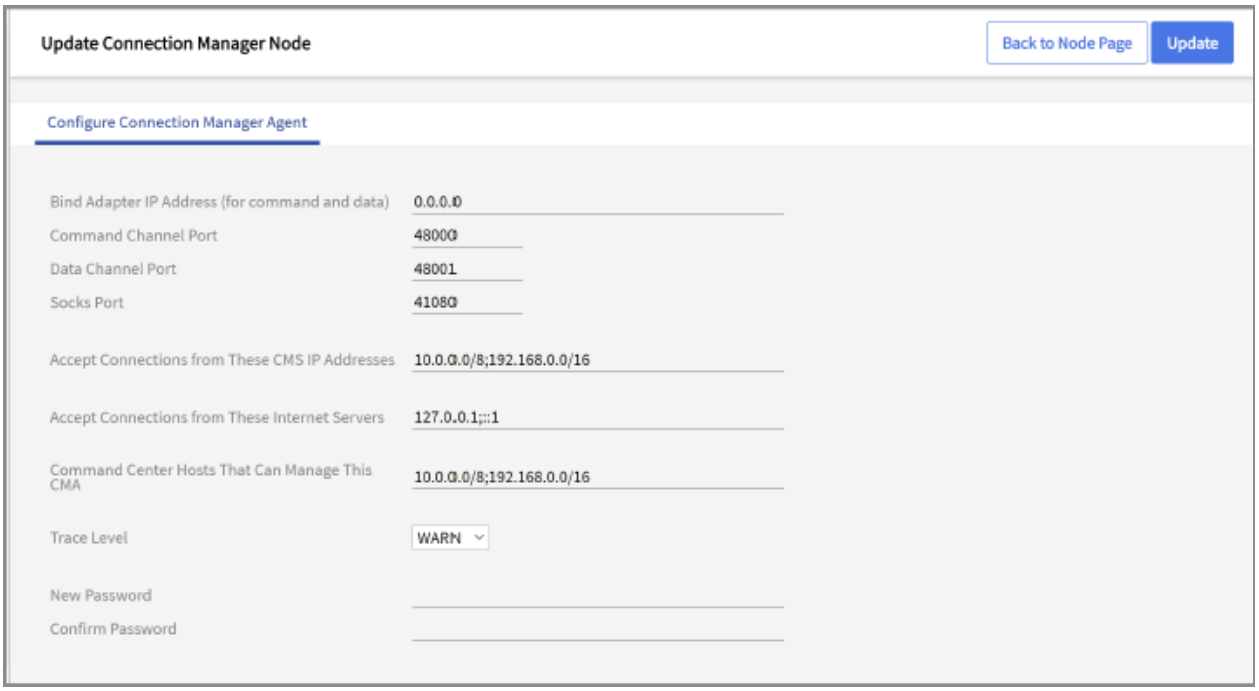
Updating CMA Configuration Information

After clicking **SampleCMA**, the Update Connection Manager Node page is displayed with the information entered on the Add Connection Manager Node page.



You can click **Update** to update the connectivity information for this CMA.

You can click **Retrieve Config** to retrieve the Connection Manager configuration parameters for this node. The following page is displayed.



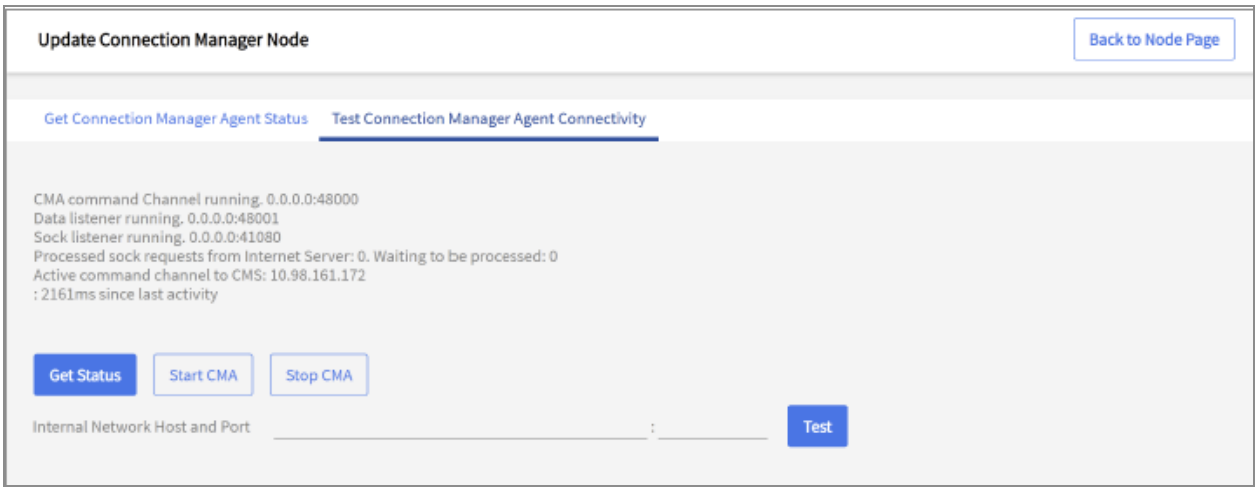
This page displays the configuration information for the Connection Manager node. You can update parameters and click **Update Config** to update the configuration.

If you update the **New Password** field, make sure to update the password on the Update Connection Manager Node page.

If you want to use the **Get Status > Test** function, make sure that the **Accept Connections from These Internet Servers** field is configured to accept changes from 127.0.0.1 and ::1, in addition to the IP addresses of the Internet Server instances. tests are initiated from the TCP Loopback address (127.0.0.1).

Note: When updating the **Command Center Hosts That Can Manage This CMA** field, make sure that you correctly define the IP address or subnet of . Otherwise, you might be unable to manage the Connection Manager node through . If this happens, you need to update the configuration `.xml` file described in Connection Manager Configuration Files and then manually restart the CMA server.

When you click **Get Status**, the following page is displayed showing the current status of the Connection Manager node.



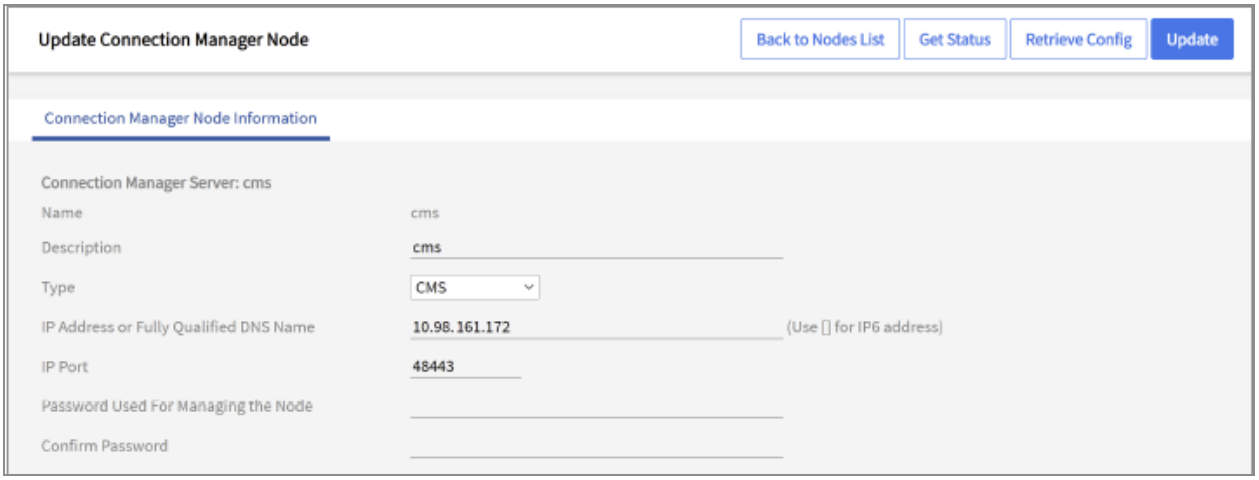
On this page, you can perform the following functions:

- **Get Status**: updates the CMA status.
- **Start CMA**: starts the CMA server.
- **Stop CMA**: stops the CMA server.
- **Test**: tests whether a connection to an internal server is available through Connection manager.

  Enter an IP name or IP address and the IP port and click **Test**. A message is displayed showing whether a connection can be established to this remote server.

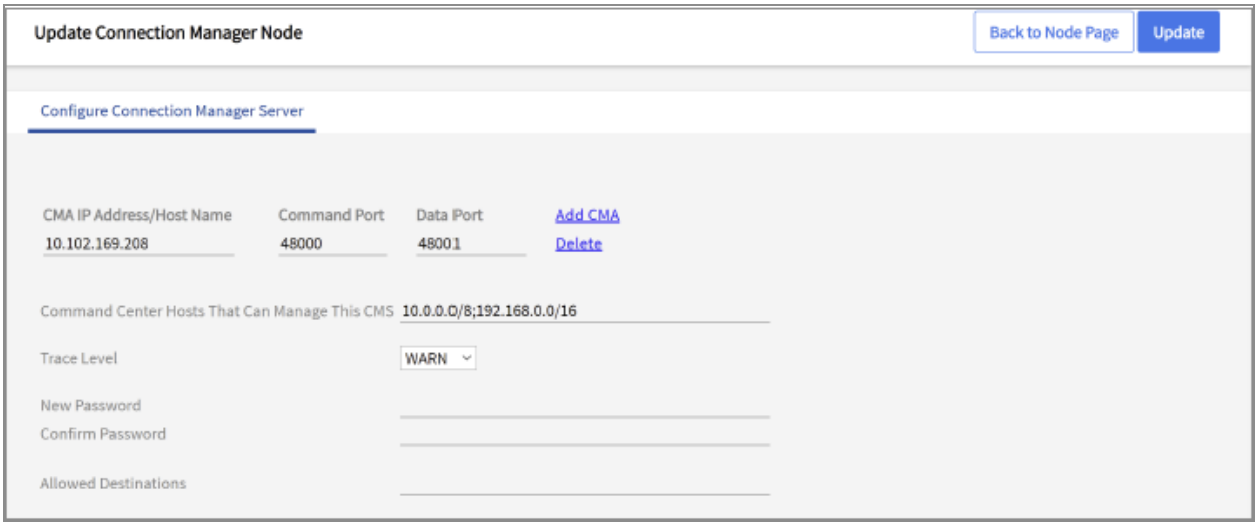
Updating CMS Configuration Information

After clicking **SampleCMS**, the Update Connection Manager Node page is displayed with the information entered on the Add Connection Manager Node page.



You can click **Update** to update the connectivity information for this CMS.

You can click **Retrieve Config** to retrieve the Connection Manager configuration parameters for this node. The following page is displayed.



This page displays the configuration information for the Connection Manager node. You can update parameters and click **Update Config** to update the configuration.

If you update the **New Password** field, make sure to update the password on the Update Connection Manager Node page.

Note: When updating the **Command Center Hosts That Can Manage This CMS** field, make sure that you correctly define the IP address or subnet of . Otherwise, you might be unable to manage the Connection Manager node through . If this happens, you need to update the configuration `.xml` file described in Connection Manager Configuration Files and then manually restart the CMS server.

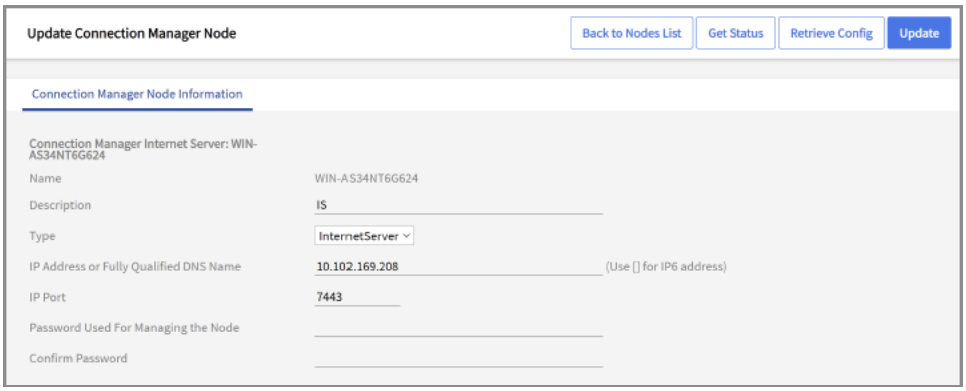
When you click **Get Status**, the following page is displayed showing the current status of the Connection Manager node.

On this page, you can perform the following functions:

- **Get Status**: updates the CMS status.
- **Start CMS**: starts the CMS server.
- **Stop CMS**: stops the CMS server.

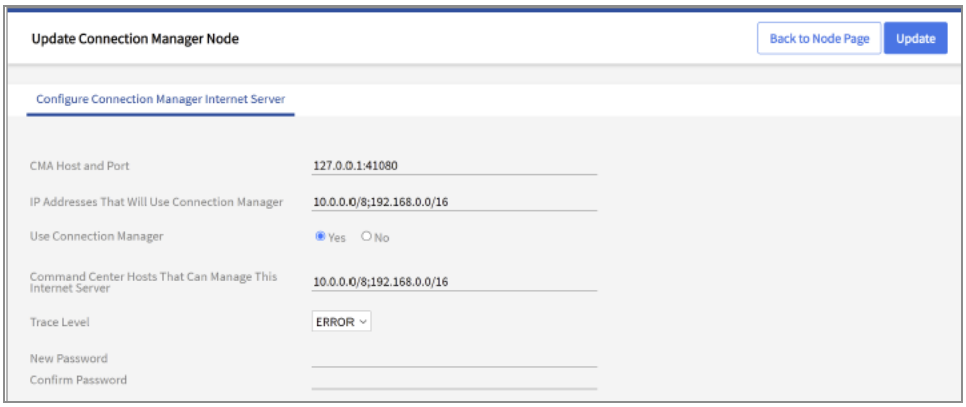
Updating Internet Server Configuration Information

After clicking **SampleIS**, the Update Connection Manager Node page is displayed with the information entered on the Add Connection Manager Node page.



You can click **Update** to update the connectivity information for this Internet Server.

You can click **Retrieve Config** to retrieve the Connection Manager configuration parameters for this node. The following page is displayed.



This page displays the configuration information for the Connection Manager node. You can update parameters and click **Update Config** to update the configuration.

If you update the **New Password** field, make sure to update the password on the Update Connection Manager Node page.

Note: When updating the **Command Center Hosts That Can Manage This Internet Server** field, make sure that you correctly define the IP address or subnet of . Otherwise, you might be unable to manage the Connection Manager node through . If this happens, you need to update the configuration `.xml` file described in Connection Manager Configuration Files and then manually restart Internet Server.

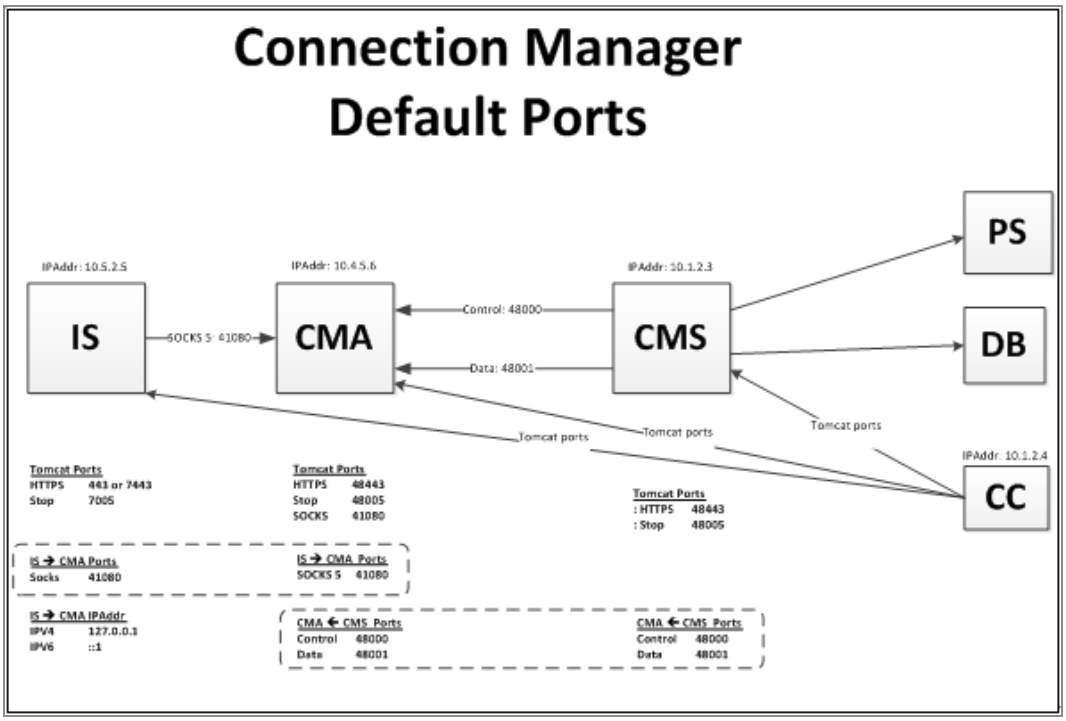
When you click **Get Status**, the following page is displayed showing the current status of the Connection Manager node.

On this page, you can perform the following function:

- **Get Status**: updates the Internet Server status.

Connection Manager Ports

The following figure shows the ports and IP addresses used in a simple Connection Manager installation.



Note: The TCP ports shown in the figure above are the default ports as configured when CMA and CMS are installed.

Internet Server

When an Internet Server requires a connection to the internal network, it makes a connection to CMA over port 41080.

During Internet Server initialization, Internet Server listens on one HTTPS port (443 or 7443) and waits for connections to configure the Internet Server Connection Manager properties.

When you use it to configure the Internet Server Connection Manager properties, make a connection to the Internet Server HTTPS port (typically 443 or 7443).

CMA

During the CMA initialization, CMA listens on the following four ports:

- 41080: waits for connection requests from Internet Server.
- 48443: waits for connections from to configure the CMA properties.
- 48000: waits for CMS control channel connections.
- 48001: waits for CMS data connections (requested by CMA over the CMS control channel).

CMS

During the CMS initialization, CMS listens on one port (48443) and waits for connections to configure the CMS properties.

At Initialization, and each time a new CMA is activated or a CMA connection is lost, CMS attempts to connect to CMA port 48000. If this connection fails, CMS waits for 30 seconds and tries again.

When CMA requests a connection from CMS, CMS connects to the remote server (for example, Oracle DB server). After that connection is completed, CMS connects to the CMA server on port 48001 (data connection port).

Command Center

Command Center communicates with Internet Server, CMA, and CMS servers to configure the Connection Manager properties:

- CMA: using port 48443.
- CMS: using port 48443.
- Internet Server: using port 443 or 7443.

Firewall Considerations

You must conform to the following firewall rules for Connection Manager to operate correctly:

- must be able to open TCP connections to CMS, CMA, and Internet Server.

  CMS generally executes in the internal network on port 48443; CMA generally executes in the DMZ on port 48443; Internet Server generally executes in the DMZ on port 443 or 7443.

  If these ports are not opened, Connection Manager can still operate but you cannot use it to configure the Connection Manager nodes. Normal and Internet Server definitions still work. But if you want to change the ports on a CMA or Internet Server, you must make the changes directly to the .xml configuration files. For more information on the configuration files, see Connection Manager Configuration Files.
- CMS must be able to open TCP connections to CMA on ports 48000 and 48001. If not, the Connection Manager does not work.
- Internet Server must be able to open TCP connections to CMA on port 41080. If not, the Connection Manager does not work.
- CMS must be able to open TCP connections to internal servers. If not, the Connection Manager requests does not work on this server.
- Server shutdown ports (generally 48005) do not have to be allowed by the firewall. Internet Server, CMA, and CMS shutdown ports are typically used by shutdown scripts executing on the instance where the Internet Server, CMA, or CMS server is executing.
- When a connection is active between a CMS and a CMA, CMA initiates heartbeat requests to CMS every 45 seconds. If a response is not received within 45 seconds, CMA breaks the connection to CMS and waits for CMS to establish a new connection to CMA.

Connection Manager Configuration Files

You can use a text editor to configure the Connection Manager parameters saved in the CMS, CMA, and Internet Server configuration files.

Note: Use a text editor to configure the CMA, CMS, and Internet Server configuration files only when you cannot use to configure these files.

CMS Configuration File

The CMS configuration file is located in the `<CMS_Install>/server/webapps/commgr/WEB-INF/reverseProxyInternal.xml` directory.

Note: It is good practice to update this file only when directed to or when you cannot use to manage CMS.

A sample CMS configuration file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<proxy-config>
  <!-- internal proxy settings -->
  <internal-proxy>
  <!-- command channel settings -->
  <command-channels max-inactive="90">
  <!-- timeout and retry interval to setup command channel to DMZ proxy
-->
   <connection-setup retry-interval="30" timeout="20"/>
   <!-- DMZ proxy hosts info to which to build command channel -->

   <!--
     <channel>
     <address>specifyDMZServiceAddr2</address>
     <command-port>48000</command-port>
     <data-port>48001</data-port>
     </channel>
      -->
<channel>
<address>10.1.2.3.</address>
<command-port>48000</command-port>
<data-port>48001</data-port>
</channel>

   </command-channels>

   <!-- data channel settings -->
   <data-channel>
    <!-- timeout to set up data channel to DMZ proxy -->
    <connection-setup timeout="45"/>
    </data-channel>

     <!-- socks settings -->
     <socks>
```

```
      <!-- timeout to finish connecting to final destination -->
      <connection-setup timeout="45"/>
       </socks>

        <!-- which machines can manage this CMS -->
        <proxy-manage>
        <valid-hosts>10.0.0.0/8;192.168.0.0/16</valid-hosts>
        <password>xxxxxxxxxxxxxxxxxxxxxxx </password>
        </proxy-manage>

<!-- allowed final destinations. e.g. 10.97.196.100, 10.97.196.100/8,
10.97.196.100/8:21, 10.97.196.100/8:5000-5500. Empty means allow all -->
<allowed-dest/>
    </internal-proxy>
</proxy-config>
```

CMS Configuration Parameters

The CMS configuration parameters are as follows.

command-channels

- `max-inactive`: defines the amount of time that a command channel remains inactive before terminating the connection. The default value of 90 indicates that CMS waits for up to 90 seconds before terminating the connection to CMA. CMS then attempts to re-establish the control connections to the control channel every 30 seconds (depending on the value of `retry-interval`).
- `retry-interval`: defines how frequently CMS attempts to establish a connection to CMA when the connection to the CMA command channel is down.
- `timeout`: defines the timeout for TCP connection establishment to the control channel.

channel

Defines each CMA to which CMS connects. Define a channel for each CMA.

- `address`: defines the CMA IP address or IP name.
- `command-port`: defines the IP port for command (namely control) connections to

CMA. CMA must be configured to listen on this port.

- `data-port`: defines the IP port for data connections to CMA. CMA must be configured to listen on this port.

data channel

- `connection-setup-timeout`: defines the timeout for TCP connection establishment to the data channel.

socks

`connection-setup-timeout`: defines the timeout for TCP connection establishment to the destination (namely target) server in the internal network.

proxy-manage

- `valid-hosts`: defines the hosts that can manage this CMS. IP addresses can be specified as a full IP address or an IP address with the number of subnet bits. Multiple IP addresses can be defined by separating them with a semicolon.
- `password`: defines the encrypted management password.

allowed-dest

Defines the destination IP address or IP names and IP ports to which CMS can connect. This parameter can be defined in the following formats:

- 10.1.2.3: connections can be made to all ports on IP address 10.1.2.3.
- 10.1.2.0/24: connections can be made to all ports on subnet 10.1.2.0.
- SQLServer1:1433: connections can be made to IP name SQLServer1 on port 1433.
- FTPServer:40000-40100: connections can be made to the IP name FTPServer on ports 40000-40100.

CMA Configuration File

The CMA configuration file is located in the `<CMA_Install>/server/webapps/commgr/WEB-INF/reverseProxyDmz.xml` directory.

Note: It is good practice to update this file only when directed to by TIBCO Technical Support or when you cannot use to manage CMA.

A sample CMA configuration file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<proxy-config>

   <!-- DMZ proxy settings -->
  <dmz-proxy>
   <!-- command channel settings -->
    <command-channel>
    <!-- address and port to accept command channel request from
internal RP proxy -->
   <listener handshake-timeout="20" keep-alive="45" keep-alive-
timeout="30">
          <address>0.0.0.0</address>          <!-- empty means 0.0.0.0 -
->
                <port>48000</port>
   </listener>
     <!-- valid hosts from which to accept command channel -->
    <valid-internal-hosts>10.0.0.0/8;192.168.0.0/16</valid-internal-
hosts>
     </command-channel>

     <!-- data channel settings -->
     <data-channel>
     <!-- address and port to accept data channel request from internal
RP proxy -->
      <listener>
         <address>0.0.0.0</address>           <!-- empty means 0.0.0.0 -
->
          <port>48001</port>
      </listener>
       <data-pipe connect-timeout="45" idle-timeout="1800"/>
       </data-channel>

    <!-- SOCKS channel settings -->
       <socks-channel>
         <!-- address and port to accept sock5 request -->
          <listener>
            <address>0.0.0.0</address>           <!-- empty means
0.0.0.0 -->
                <port>41080</port>
```

```
            </listener>
            <!-- valid hosts from which to accept sock5 requests, can
use ; to separate multiple hosts -->
            <valid-sock5-hosts>127.0.0.1;::1</valid-sock5-hosts>
         </socks-channel>

               <proxy-selector state="cma">
<!-- state: on|off|cma, on|off are used by MFT's sock selector, cma
means this config is for cma, not for mft -->
       <internaladdress>10.0.0.0/8;192.168.0.0/16</internaladdress>

      <!-- CMA's sock server end point. use: host:port[;host:port]
format -->
       <socks-servers loadBalance="no">127.0.0.1:41080</socks-servers>
               </proxy-selector>

       <!-- which machines can manage this CMA -->
       <proxy-manage>
        <valid-hosts>10.0.0.0/8;192.168.0.0/16</valid-hosts>
               <password>xxxxxxxxxxxxxxxxxxxxxxx </password>
       </proxy-manage>

    </dmz-proxy>

</proxy-config>
```

CMA Configuration Parameters

The CMA configuration parameters are as follows.

command-channel

- `handshake-timeout`: defines how long CMA waits for the handshake to complete.
- `keep-alive`: defines how frequently CMA issues heartbeat requests to CMS. The default value of 45 indicates that CMA sends heartbeat requests to CMS every 45 seconds during periods of inactivity.
- `keep-alive-timeout`: defines the number of seconds that CMA waits for heartbeat response from CMS before closing the connection.
- `address`: defines the adapter IP address that CMA binds to before listening for incoming control channel requests. The default value of 0.0.0.0 indicates using all

adapter IP addresses.

- `port`: defines the IP port that CMA listens on for incoming control channel connections.
- `valid-internal-hosts`: defines IP addresses of internal CMS servers. IP addresses can be specified as a full IP address or an IP address with the number of subnet bits. Multiple IP addresses can be defined by separating them with a semicolon.

data-channel

- `address`: defines the adapter IP address that CMA binds to before listening for incoming data channel requests. The default value of 0.0.0.0 indicates using all adapter IP addresses.
- `port`: defines the IP port that CMA listens on for incoming data channel connections.
- `connect-timeout`: defines how long CMA waits for a CMS connection requested by CMA over the command (namely control) channel.
- `idle-timeout`: this parameter is for future use and can be ignored.

socks-channel

- `address`: defines the adapter IP address that CMA binds to before listening for incoming requests from Internet Server. The default value of 0.0.0.0 indicates using all adapter IP addresses.
- `port`: defines the IP port that CMA listens on for incoming connections from Internet Server.
- `valid-sock5-hosts`: defines the Internet Server hosts from which CMS accepts connection requests. The default value of 127.0.0.1 indicates accepting requests from the local host. Multiple IP addresses can be defined by separating them with a semicolon.

proxy-manage

- `valid-hosts`: defines the hosts that can manage this CMS. IP addresses can be specified as a full IP address or an IP address with the number of subnet bits. Multiple IP addresses can be defined by separating them with a semicolon.
- `password`: defines the encrypted management password.

Internet Server Configuration File

The Internet Server Connection Manager configuration file is located in the `<MFTIS_Install>/server/webapps/cfcc/reverseProxyDmz.xml` directory.

Note: It is good practice to update this file only when directed to by TIBCO Technical Support or when you cannot use the user interface to manage the Connection Manager component of Internet Server.

A sample Internet Server Connection Manager configuration file is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<proxy-config>

<!-- DMZ proxy settings -->
<dmz-proxy>

   <!-- command channel settings -->
       <command-channel>
       <!-- address and port to accept command channel request from
internal RP proxy -->
       <listener handshake-timeout="20" keep-alive="45" keep-alive-
timeout="30">
       <address>0.0.0.0</address>          <!-- empty means 0.0.0.0 -->
       <port>48000</port>
       </listener>
       <!-- valid hosts from which to accept command channel -->
         <valid-internal-hosts>10.0.0.0/8;192.168.0.0/16</valid-
internal-hosts>
        </command-channel>

    <!-- data channel settings -->
    <data-channel>
    <!-- address and port to accept data channel request from internal
RP proxy -->
       <listener>
        <address>0.0.0.0</address>        <!-- empty means 0.0.0.0 -->
        <port>48001</port>
        </listener>
            <data-pipe connect-timeout="45" idle-timeout="1800"/>
        </data-channel>

        <!-- SOCKS channel settings -->
        <socks-channel>
```

```
          <!-- address and port to accept sock5 request -->
          <listener>
           <address>0.0.0.0</address>         <!-- empty means 0.0.0.0 -
->
           <port>41080</port>
          </listener>
      <!-- valid hosts from which to accept sock5 requests, can use ; to
separate multiple hosts -->
        <valid-sock5-hosts>127.0.0.1;::1</valid-sock5-hosts>
        </socks-channel>

<proxy-selector state="on"> <!-- state: on|off|cma, on|off are used by
MFT's sock selector, cma means this config is for cma, not for mft -->
 <internaladdress>10.0.0.0/8;192.168.0.0/16;1.2.3.4/32</internaladdress>

       <!-- CMA's sock server end point. use: host:port[;host:port]
format -->
       <socks-servers loadBalance="no">10.1.2.3:41080</socks-servers>
       </proxy-selector>

       <!-- which machines can manage this CMA -->
       <proxy-manage>
       <valid-hosts>10.0.0.0/8;192.168.0.0/16</valid-hosts>
               <password>xxxxxxxxxxxxxxxxxxxxxxx </password>
       </proxy-manage>
    </dmz-proxy>

</proxy-config>
```

Internet Server Configuration Parameters

The Internet Server configuration parameters are as follows.

proxy-selector

- `internaladdress`: defines the target IP addresses that Internet Server routes through CMA. IP addresses can be specified as a full IP address or an IP address with the number of subnet bits. Multiple IP addresses can be defined by separating them with a semicolon.

socks-server

- `ipaddresses`: defines the IP addresses and IP ports of the CMA servers. Use the format of IPAddress:port when defining this parameter. Multiple CMA servers can be defined by separating the IP addresses with a semicolon.
- `load-balance`: this parameter is for future use and can be ignored.

proxy-manage

- `valid-hosts`: defines the hosts that can manage this Internet Server. IP addresses can be specified as a full IP address or an IP address with the number of subnet bits. Multiple IP addresses can be defined by separating them with a semicolon.
- `password`: defines the encrypted management password.

Configuring Internal Clients

When an Internet Server establishes connections to internal servers, the TCP connection uses the IP address of Internet Server. Therefore, the internal server detects that the Internet Server initiates the connection request. When using Connection Manager, CMS initiates the TCP connection to the internal server. The internal server detects that CMS initiates the connection request. Therefore, whenever an internal server is configured to accept connections from a particular IP address, you must configure the CMS IP address instead of the Internet Server IP address.

Platform Server

When Platform Server is configured to Require Node Definitions or is using responder profiles, you must create a node definition for each CMS server that can connect to Platform Server. Additionally, if you are using responder profiles, you must add a responder profile for each CMS node definition.

Database Servers

If database servers are configured to accept connections from particular Internet Servers, the database must be configured with the IP addresses or IP names of all of the defined CMS servers that can connect to this database server.

Best Practices

For best results, follow the following guidelines when implementing the Connection Manager:

- Use the default ports whenever possible when installing and testing Connection Manager. These ports are used only by Connection Manager and are not used by external clients. Firewalls must be configured to prohibit external client access to these ports. If you want to change the ports, make changes one at a time and test the change before changing additional ports.
- Use the default configuration to start testing. The default configuration is very generic and can work in most environments. If you want to lock down Connection Manager, make one change at a time and test this change before making additional changes.
- When adding a Connection Manager CMA, CMS, or Internet Server, always use the **Test** button to verify the connectivity information and password. This ensures it can communicate with the Connection Manager node.
- Use the **Get Status** button to determine the status of CMA, CMS, and Internet Server.
- Get simple Connection Manager connectivity working before configuring more complicated high availability or high availability Connection Manager connectivity.
- After installation, you can use the CMA **Get Status > Test** buttons to test connectivity to the target server in the internal network.

Debugging

Follow the following steps to debug Connection Manager:

1. Make sure that you configure the Connection Manager CMA, CMS, and Internet Server nodes with the correct connectivity information and password. On the Add Connection Manager Node page, click the **Test** button to verify that the connectivity information is correct.
2. Verify that the firewall ports are opened as defined in the Firewall Considerations.
3. Use to configure Internet Server, CMA, and CMS. If you cannot retrieve configuration,

a message is displayed to show the error. If you receive a connection error, check the following things:

- Verify that the firewall has been opened for the necessary ports.
- Verify that the IP address and IP port have been configured correctly.
- Issue a `NETSTAT` command on the Connection Manager node to make sure the Connection Manager node is listening on the defined port.

4. If you have connectivity to the Connection Manager nodes, but connections fail, use the CMA **Get Status > Test** function. This function tests whether CMA can access the defined internal server. tests are initiated from the CMA TCP Loopback address (127.0.0.1); therefore, make sure that the CMA **Accept Connections from These Internet Servers** field is configured to accept changes from 127.0.0.1 and ::1, in addition to the IP addresses of the Internet Server computers. Otherwise, tests initiated from fail with an error indicating that CMA will not accept requests from the local host.
5. Tracing can be configured to assist in debugging. For CMA and CMS, the default tracing is INFO; for Internet Server, the default tracing is ERROR. This writes trace files to the following directories:

   - CMA: `<CMA_Install>/bin/RPLog.txt`
   - CMS: `<CMS_Install>/bin/RPLog.txt`
   - Internet Server: `<MFTIS_Install>/server/logs/catalina.out`

   Generally speaking, look at the CMS tracing first. The CMS tracing documents problems in connecting to CMA.

Appendix C: Antivirus Support

Internet Server supports antivirus checking through the ICAP interface implemented by an antivirus software provider. MFT does not distribute antivirus software. The customer is responsible for installing the antivirus software and configuring and starting the ICAP interface. Since antivirus is a global parameter, you must make sure that all Internet Server instances have connectivity to the ICAP interface port.

MFT has been tested with two ICAP software products:

- Symantec Protection Engine
- Squid/Clam

The antivirus interface has been coded so that other antivirus products can be configured to work with Internet Server.

Note: Transferring large files with virus scanning enabled slows down transfer throughput and increases CPU utilization. All files are scanned by default. You should use a REGEX to limit the scan to only a certain type of file. Since every data packet is sent to the target ICAP server, the ICAP server must be on the same network as the Internet Server instances with a high-speed connection and low latency.

Antivirus Modes

Internet Server supports the following two Antivirus modes.

- Streaming
- Store and Forward

The mode can be set globally and can be overridden for individual transfers and servers. Different transfers can use different antivirus modes. The mode that you select for a transfer depends on the client you are using, the target server used for a transfer and whether the transfer is for an upload or download.

Streaming

As packets are received, Internet Server writes the packets to the ICAP server and to the destination (client for a download and server for an upload). When the Internet Server detects a virus, the transfer terminates with an error. The downside to streaming mode is that by the time a virus is detected, the virus file is transferred to the target server. Internet Server initiates a request to delete the file. However, there are some target servers where there is no mechanism to delete a file. For example, if you send a file to an HTTP Server, there is no way to delete the file. The advantage of streaming mode is that transfers normally execute seamlessly and there is no effect on transfer clients or servers.

When should you use **Streaming** mode?

- When Platform Server is initiating a download
- When uploading files to target servers that can delete files or can detect that a transfer failed.

Store and Forward

As packets are received, Internet Server sends the packets to the ICAP Server, encrypts the packets, and writes the packets to a temp disk file. When the entire file is received, virus checking is completed, and no virus is found, Internet Server decrypts the file and sends the data packets to the target server. If a virus has been detected, the transfer terminates with an error. The disadvantage of **Store and Forward** mode is that some clients (ex: FTP or SFTP clients) experience a timeout when waiting for the staged file to be sent to the ICAP server and to the target Server. The advantage of **Store and Forward** mode is that the virus is not sent to the target. Internet Server detects the virus before sending the file to the target.

When should you use **Store and Forward** mode?

- When using a client that may not detect a file transfer and delete a file. For example, FTP, SFTP, and HTTP clients do not delete a file if a virus is detected during a download.
- When uploading files to target servers that cannot delete files or cannot detect that a transfer failed. For example, when transferring to HTTP or HDFS.

Enabling Antivirus

To enable antivirus, complete the following steps.

Procedure

1. Go to **Configuration > System Configuration**.
2. Click the **Anti Virus Settings** tab.

Antivirus Settings Fields

For more information on each field, see the Admin help page.

Field	Description
Enabled	Defines whether antivirus is enabled or disabled. Note that when antivirus is disabled, the antivirus tabs on the **Server** and **Transfer** definitions are not displayed.
AV Software	Allows you to select the ICAP server Type. Current options are: • `Symantec Protection Engine` • `Squid/Clam` • `Other` We recommend using `Other` when a different ICAP server is used.
ICAP Server Host Name	Defines the IP Name or IP Address of the target ICAP server.
ICAP Server Port	Defines the IP Port of the target ICAP Server. Note that when you click **use TLS**, the port is set to `11344` and when this checkbox is unselected, the port is set to `1344`.
Use TLS	Defines whether the ICAP interface uses TLS. Select this checkbox to use TLS when communicating to the ICAP server. We suggest using TLS to communicate to the ICAP server. But this setting depends on how the ICAP

Field	Description
	server is configured.
Upload ICAP Mode/Service Name	Defines the ICAP mode and the name of the ICAP service used when uploading a file. Supported modes are REQMOD and RESPMOD. REQMOD is the default mode. The default service names are filled in when using Symantec and Squid/Clam. You must set this only when Other is selected as the AV Software type. Your Antivirus provider documentation lists the ICAP service name.
Download ICAP Mode/Service Name	Defines the ICAP mode and the name of the ICAP service used when downloading a file. Supported modes are REQMOD and RESPMOD. RESPMOD is the default mode. The default service names are filled in when using Symantec and Squid/Clam. You must set this only when Other is selected as the AV Software type. Your Antivirus provider documentation lists the ICAP service name.
Max Scan MegaBytes	Defines the maximum number of bytes to be scanned for a virus. When this number is reached, no additional packets are scanned for a virus. Most virus scanning software has a file size limit but continues to accept packets until the end of the file is reached.
Unexpected ICAP errors	Defines what happens when an unexpected ICAP error is detected. This can be a connectivity error or an unexpected HTTP return code or packet. Valid values are: **Error Value** — **Description** Fail — The transfer terminates with an error. Continue — The transfer continues and no additional virus scanning is performed for that transfer.
Mode	Defines the mode: Streaming or Store and Forward. See Antivirus Modes for an explanation of the two modes.

Field	Description
Virus Email Notification	Defines one or more email addresses (delimited by a comma) to be notified when a virus is detected.
ICAP Custom Header Name	This is the header that would indicate if the ICAP server has found a virus.
Log ICAP Messages	Defines whether a debug file is written with all ICAP Request and Response messages. Select this checkbox when you need to debug the ICAP interface.
Select Server to Test Connection	You can select an Internet Server instance where the ICAP connection can be tested. Select the Internet Server instance and click the "Test" button. Internet Server connects to the ICAP server and sends an HTTP packet to the ICAP server. Always test all Internet Server instances before configuring Servers or Transfers to perform antivirus scanning. This makes sure there is connectivity to the ICAP server.

Enabling ICAP Scanning File Transfers

There are two ways to enable ICAP Scanning for file transfers.

1. Enable Antivirus scanning on the Server definition
2. Enable Antivirus scanning on the Transfer definition

Note: Antivirus settings on the Transfer definition override the Antivirus definitions on the Server definition. By default, the Transfer definition uses the antivirus settings from the server definition.

Enabling Antivirus Scanning on Server Definitions

To enable antivirus scanning on Server definitions, complete the following steps.

Procedure

1. Go to **Partners > Servers > Add Server**.

2. Click the **Anti Virus Properties** tab.
3. Enter the required information described in the table below.

Field	Description
Transfer Scan Direction	Defines whether the antivirus checking us performed on uploads and/or downloads. Select the **Upload** checkbox to enable Antivirus checking for uploads. Select the **Download** checkbox to enable antivirus checking for downloads.
Mode	Defines the antivirus mode. See Antivirus Modes for an explanation of the two modes.
Upload Scan File REGEX	Defines the REGEX (Regular Expression) that is used to determine if a file being uploaded is scanned. Here is an example of a regex that scans files with extensions ".exe" and ".dll" (not case sensitive). ^.*.(?-i)exe$|^.*.(?-i)dll If nothing is entered in the field, then all files are scanned.
Download Scan File REGEX	Defines the REGEX (Regular Expression) that is used to determine if a file being downloaded is scanned. Here is an example of a regex that scans files with extensions ".exe" and ".dll" (case-insensitive). ^.*.(?-i)exe$|^.*.(?-i)dll If nothing is entered in the field, then all files are scanned.

Note: The **Update Server** page has the same **Anti Virus Properties** tab.

Enabling Antivirus Scanning on Transfer Definitions

To enable antivirus scanning on Transfer definitions, complete the following steps.

Procedure

1. Go to **Transfers > Internet Transfers > Add Transfer**.
2. Click the **Anti Virus Properties** tab.

3. Enter the required information described in the table below.

Field	Description
Transfer AV Scan	Defines whether to override the server definition transfer properties. There are three options. **Option** / **Description** Yes — Scan files using this transfer definition. No — Do not scan files using this transfer definition. Server Default — Use the **Server Anti Virus** setting
Mode	Defines the antivirus mode. See Antivirus Modes for an explanation of the two modes.
Scan File REGEX	Defines the REGEX (Regular Expression) that is used to determine if a file being uploaded or downloaded is scanned. Here is an example of a regex that scans files with extensions ".exe" and ".dll" (case-insensitive). ^.*.(?-i)exe$|^.*.(?-i)dll If nothing is entered in the field, then all files are scanned.

Note: On the **Add Transfer** page, when you set the **Required Transfer Information > Transfer Direction** to `Both`, two transfer definitions are created. The parameters in the **Anti Virus Properties** tab are applied to both transfers.

Antivirus web.xml Parameters

When using **Store and Forward** mode, Internet Server writes an encrypted version of the file to a temp directory. By default, MFT writes the temp files to this directory:

```
<MFT-Install>/server/webapps/cfcc/WEB-INF/StoreAndForwardTempDir
```

If you want to override this directory, you can set the `temp` directory in the `web.xml` parameter: `AntiVirusTempDirectory`

Here is a sample that changes the temp folder to: `/tmp/mftav`.

```
<context-param>
<param-name>StoreAndForwardTempDir</param-name>
<param-value>/tmp/mftav</param-value/>
</context-param>
```

Then, restart the MFT Internet Server.

Note:

- If the directory does not exist, Internet Server creates the directory. But you must make sure that the user executing Internet Server has all access rights to the defined directory.
- The temp files are deleted when the transfer terminates.

Appendix D: Data Loss Prevention (DLP) Support

TIBCO MFT Internet Server supports DLP checking through the ICAP interface implemented by a DLP software provider. MFT does not distribute DLP software. The customer is responsible for installing the DLP software and configuring and starting the ICAP interface. Since DLP is a global parameter, ensure that all TIBCO MFT Internet Server instances have connectivity to the ICAP interface port.

MFT has been tested with Symantec Data Loss Prevention Network Monitor and Network Prevent server. The Data Leak Prevention feature is coded in such a way that it can be used with other DLP software. However, the DLP violation response can change for each DLP ICAP server; this may require a fix to support additional DLP ICAP servers.

Note: Transferring large files with DLP violation scanning enabled, slows down transfer throughput and increases CPU utilization. All files are scanned by default. Use a Regular Expression (REGEX) to limit the scan to a certain type of file. Since every data packet is sent to the target ICAP server, the ICAP server must be on the same network as the TIBCO MFT Internet Server instances with a high-speed connection and low latency.

DLP Modes

TIBCO MFT Internet Server supports the following DLP modes:

- Streaming
- Store and Forward

The mode can be set globally and overridden for individual transfers and servers. Different transfers can use different DLP modes. The mode that you select for a transfer depends on the client you are using, the target server used for a transfer, and whether the transfer is for an upload or download.

Streaming

As packets are received, TIBCO MFT Internet Server writes the packets to the ICAP server and to the destination (`client` for a download and `server` for an upload). When TIBCO MFT Internet Server detects a violation, the transfer stops with an error. The downside to streaming mode is that by the time a violation is detected, the violating file is transferred to the target server. TIBCO MFT Internet Server initiates a request to delete the file. However, some target servers do not have a mechanism to delete a file. For example, if you send a file to an HTTP server, there is no way to delete the file. The advantage of the streaming mode is that transfers normally run seamlessly and there is no effect on transfer clients or servers.

Scenarios for using Streaming Mode

- When a platform server is initiating a download.
- When uploading files to target servers that can delete files or detect that a transfer failed.

Store and Forward

As packets are received, TIBCO MFT Internet Server sends the packets to the ICAP Server, encrypts the packets, and writes the packets to a temp disk file. When the entire file is received, DLP checking is complete and no violations are found, TIBCO MFT Internet Server decrypts the file and sends the data packets to the target server. In the event of a violation, the transfer stops with an error. The disadvantage of the Store and Forward mode is that some clients (for example, FTP or SFTP) experience a timeout when waiting for the staged file to be sent to the ICAP server and the target Server. The advantage of the Store and Forward mode is that the violating file is not sent to the target. TIBCO MFT Internet Server detects the violation before sending the file to the target.

Scenarios for using Store and Forward mode

- When using a client that may not detect a file transfer and delete a file. For example, FTP, SFTP, and HTTP clients do not delete a file if a violation is detected during a

download.

- When uploading files to target servers that cannot delete files or cannot detect that a transfer failed. For example, when transferring to HTTP or HDFS servers.

Enabling DLP

To enable Data Loss Prevention, perform the following steps.

Procedure

1. On the Home page, go to **Configuration > System Configuration**.
2. Click the **Data Loss Prevention Settings** tab.

DLP Settings Field

The following table lists the DLP Settings field.

Field	Description
Enabled	Defines whether DLP is enabled or disabled. When DLP is disabled, the **DLP** tabs on the **Server** and **Transfer** definitions are not displayed.
DLP Software	You can select the DLP server type. Valid options are as follows: • `Symantec` • `Other` Use `Other` when a different DLP server is used.
ICAP Server Host Name	Defines the IP name or IP address of the target ICAP server.
ICAP Server Port	Defines the IP port of the target ICAP server. Note that when you click **Use TLS**, the port is set to 11344 and when this checkbox is cleared, the port is set to 1344.

Field	Description
Use TLS	Defines whether the ICAP interface uses TLS. Select the checkbox to use TLS when communicating with the ICAP server. However, this setting depends on how the ICAP server is configured.
Upload ICAP Mode/Service Name	Defines the ICAP mode and the name of the ICAP service used when uploading a file. Supported modes are REQMOD and RESPMOD. REQMOD is the default mode. The default service names are filled in when using the Symantec DLP Software type. You must manually set this field when `Other` is selected as the DLP Software type. Your DLP provider documentation lists the name of the ICAP service.
Download ICAP Mode/Service Name	Defines the ICAP mode and the name of the ICAP service used when downloading a file. Supported modes are REQMOD and RESPMOD. RESPMOD is the default mode. The default service names are filled in when using the Symantec DLP Software type. You must manually set this field when `Other` is selected as the DLP Software type. Your DLP provider documentation lists the name of the ICAP service.
Max Scan MegaBytes	Defines the maximum number of bytes to be scanned for a violation. When the maximum number is reached, no additional packets are scanned.
Unexpected ICAP errors	Defines what happens when an unexpected ICAP error is detected. This can be a connectivity error or an unexpected HTTP return code or packet. Valid values are as follows: **Value** — **Description** Fail — Terminates transfer with an error. Continue — Continues transfer and no additional DLP scanning is performed for that transfer.
Mode	Defines the DLP mode.

Field	Description
	The valid values are as follows: • Streaming • Store and Forward For more information about the two modes, see Appendix D: Data Loss Prevention (DLP) Support.
DLP Violation Email Notification	Defines one or more email addresses (delimited by a comma) to be notified when a DLP violation is detected.
Client IP Header Name	Defines the name of the header that contains the IP address of the client. If this field is empty, then the IP address is not sent to the ICAP server. Typically, X-Client-IP is the value used. For more information, see the DLP software provider documentation.
User Header Name	Defines the name of the header that contains the user id. If this field is empty, then the IP address is not sent to the ICAP server. Typically X-Authenticated-User is the value used. Please check your DLP software provider documentation.
Log ICAP Messages	Defines whether a debug file is written with all the ICAP Request and Response messages. Select this checkbox to debug the ICAP interface.
Select Server to Test Connection	Select an Internet Server instance where the ICAP connection can be tested. Select the Internet Server instance and click the **Test** button. Internet Server connects to the ICAP server and sends an ICAP packet to the ICAP server. **Note:** Always test all Internet Server instances before configuring Servers or Transfers to perform DLP scanning. Ensure that there is connectivity to the ICAP server.

For more information about each field, see the TIBCO MFT Admin help page.

Enabling DLP Scanning File Transfers

To enable DLP Scanning for file transfers, use either of the following ways:

- Enable DLP scanning on the Server definition
- Enable DLP scanning on the Transfer definition

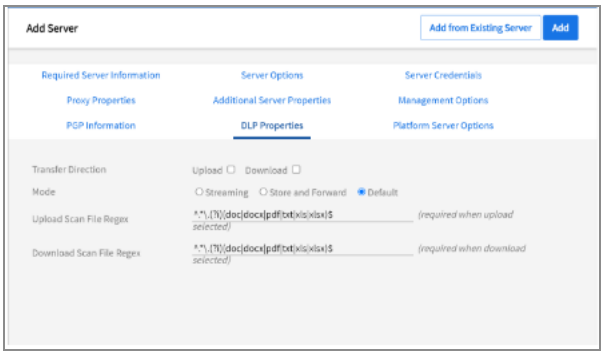
DLP settings on the **Transfer** definition override the DLP settings on the **Server** definition. By default, the **Transfer** definition uses the DLP settings from the **Server** definition.

Enabling DLP Scanning on Server Definitions

To enable antivirus scanning on **Server** definitions, complete the following steps.

Procedure

1. On the Home page, go to **Partners > Servers > Add Server**.
2. Click the **DLP Properties** tab. The following tab is displayed.



3. Enter the required information described in the following table:

Field	Description
Transfer Direction	Defines the DLP mode. For more information about the two modes, see Appendix D: Data Loss Prevention (DLP) Support.
Upload File	Defines the REGEX that is used to determine if a file being uploaded is

Field	Description
Regex	scanned. Here is an example of a REGEX that scans files with extensions ".doc", ".docx", “.pdf”, “.txt”, “.xls” or “.xlsx” (not case sensitive). ^.*\.(?i)(doc|docx|pdf|txt|xls|xlsx)$
Download File Regex	Defines the REGEX that is used to determine if a file being downloaded is scanned. Here is an example of a REGEX that scans files with extensions ".doc", ".docx", “.pdf”, “.txt”, “.xls” or “.xlsx” (not case sensitive). ^.*\.(?i)(doc|docx|pdf|txt|xls|xlsx)$

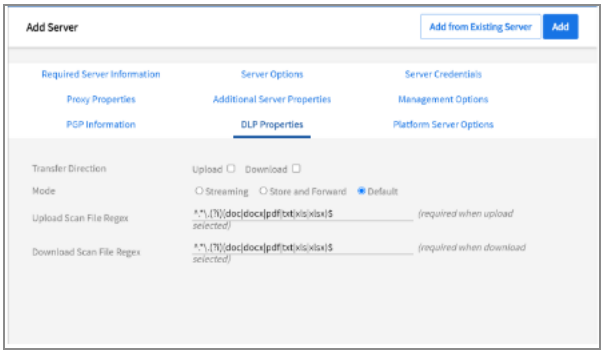
Note: The **Update Server** page has the same **DLP Properties** tab.

Enabling DLP Scanning on Transfer Definitions

To enable antivirus scanning on **Transfer** definitions, complete the following steps.

Procedure

1. On the Home page, go to **Transfers > Internet Transfers > Add Transfer**.
2. Click the **DLP Properties** tab. The following tab is displayed.



3. Enter the required information described in the following table:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Transfer DLP Scan</td><td>Defines whether to override the server definition transfer properties.

The options are as follows:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Yes</td><td>Scan files using this transfer definition.</td></tr><tr><td>No</td><td>Do not scan files using this transfer definition.</td></tr><tr><td>Server Default</td><td>Use the server DLP setting.</td></tr></table></td></tr>
<tr><td>Mode</td><td>Defines the DLP mode.

For more information about the two modes, see Appendix D: Data Loss Prevention (DLP) Support.</td></tr>
<tr><td>Scan File Regex</td><td>Defines the REGEX that is used to determine if a file being uploaded or downloaded is scanned. Here is an example of a REGEX that scans files with extensions ".doc", ".docx", “.pdf”, “.txt”, “.xls” or “.xlsx” (not case sensitive). ^.*\.(?i)(doc|docx|pdf|txt|xls|xlsx)$</td></tr>
</table>

Note: On the **Add Transfer** page, when you set the **Required Transfer Information > Transfer Direction** to `Both`, two transfer definitions are created. The parameters in the **DLP Properties** tab are applied to both transfers.

DLP web.xml Parameters

When using Store and Forward mode, TIBCO MFT Internet Server writes an encrypted version of the file to a temp directory. By default, MFT writes the temp files to this directory:

```
<MFT-Install>/server/webapps/cfcc/WEB-INF/tempstore
```

To override this directory, set the temp directory in the web.xml parameter: `StoreAndForwardTempDir`

Here is a sample that changes the temp folder to `/tmp/mftdlp`.

```
<context-param>
<param-name>StoreAndForwardTempDir</param-name> <param-
value>/tmp/mftdlp</param-value/>
</context-param>
```

Then, restart the TIBCO MFT Internet Server.

Note:

- If the directory does not exist, TIBCO MFT Internet Server creates the directory. Ensure that the user running TIBCO MFT Internet Server has all access rights to the defined directory.
- The temp files are deleted when the transfer terminates.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

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

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

Product-Specific Documentation

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

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

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to TIBCO Support website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

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

Legal and Third-Party Notices