TIBCO® Managed File Transfer Command Center

User Guide

Version 8.7.0 | October 2025

Contents

Activation

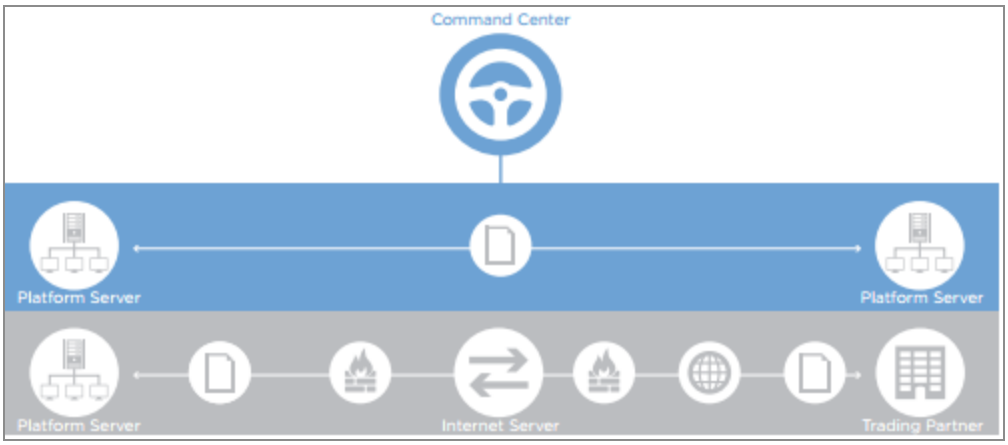
MFT Command Center requires activation using a license to start. Licenses can be generated from the TIBCO Software Downloads site at https://www.tibco.com/downloads. For complete details on activating TIBCO products, see the TIBCO Activation Service documentation at https://docs.tibco.com/products/tibco-activation-service. Activation can be configured when installing MFT Command Center. For more information, see the TIBCO® Managed File Transfer Command Center Installation.

Important: MFT Platform Server shuts down when your product entitlement ends and does not restart until you replace the license file with one that has a new entitlement end date. Replace your license file before the entitlement end date to avoid business disruption. For details on monitoring for entitlement expirations, see License Expiration Warnings

Product Overview

TIBCO® Managed File Transfer Command Center 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 Command Center provides the following benefits:

- **Centralized management**

  Browser-based, single-point-of-control for all enterprise file-transfer activities.

- **Security**

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

- **Multi-Protocol**

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

- **Full audit and reporting**

  A full suite of online inquiry tools for powerful audit and reporting functionality.

- **Delegated administration**

  Users empowered based on their role within the organization.

- **High availability and clustering**

  Support for clustering for failover and reliability.

- **Real-time alerts**

  Messages and alerts sent via JMS or email.

Administrator Browser Configuration

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

Accessing the Administrator Browser

After installing and configuring TIBCO MFT Command Center, 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 8443.

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

   `https://HostName:Port/admin`

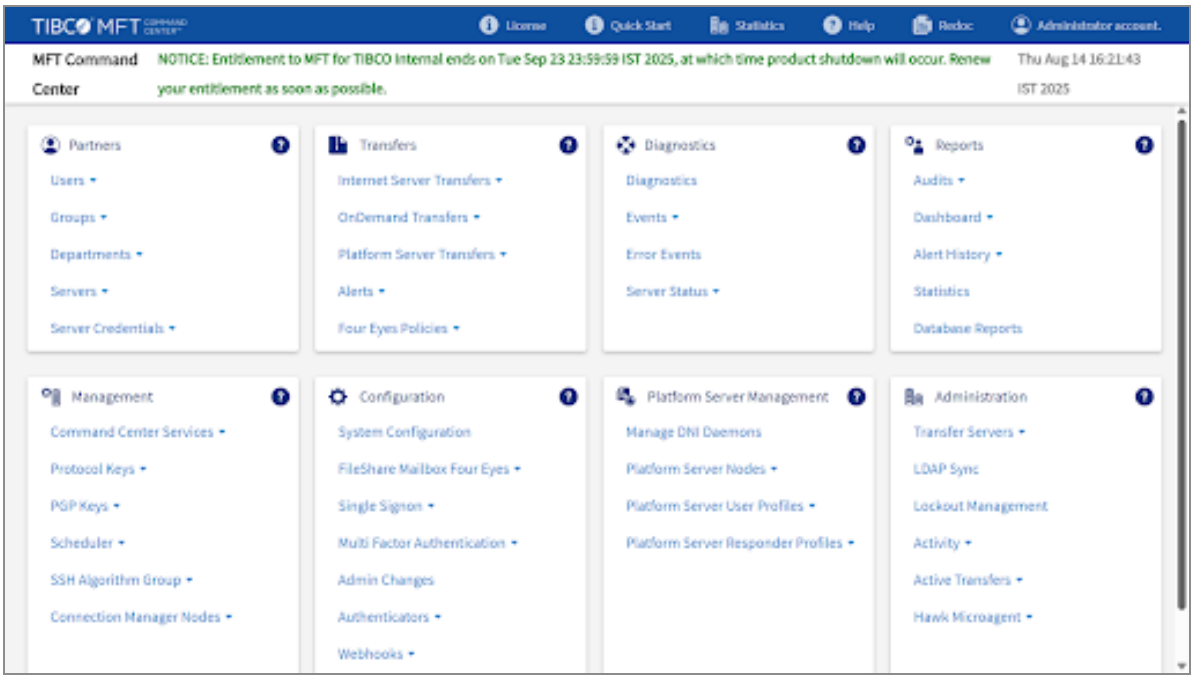
2. Enter the administrator default username and password.

   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 Command Center 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 Command Center

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 that you are accessing and all parameters on the page. This is displayed on all admin pages.

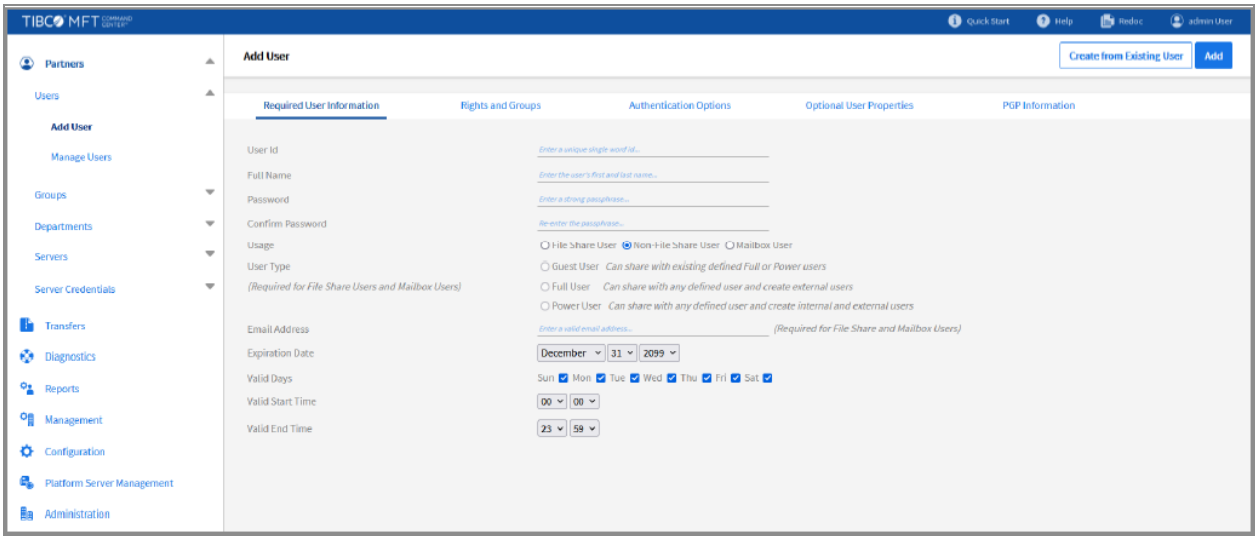
Icon/Tab	Description
	Note: This guide provides general information about the admin pages. Detailed information is provided on the help pages.
Redoc	Displayed on the upper-right side of the page. This tab displays the pane containing the links to view the API documentations for REST calls.
Administrator account	Displayed on the upper-right side of the page. Click the **Administrator account** tab to change your password or to sign out.
License	Displayed on all pages. Click the **License** tab to access the license Information.

On the landing page, you can click 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 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.
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 new users. 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.

Tab	Description
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
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 Keys, Protocol Keys, or Tags for this user. After clicking the link, the following tabs are displayed.

Tab	Description
PGP Public Keys	Defines the required parameters that you must enter to add a PGP Public Key.
Protocol Public Keys	Defines the required parameters that you must enter to add a Protocol Public Key.
Tags	Defines the required parameters that you must enter to add a tag.

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.
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.

Tab	Description
	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.
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.
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`.

Task	Description
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 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

Task	Description
	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 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

Task	Description
	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.
Four Eyes Options	Defines options that can be set when files are sent as Four Eyes attachments. You can define several options, including default sender email address, maximum attachment size, and default expiration.

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 the **Add Server** button, an info message pops up that allows you to create PGP Keys, Protocol Keys, or Tags for this Server. After clicking the link provided in the info message, the following tabs are displayed.

Tab	Description
PGP Public Keys	Defines the required parameters that you must enter to add a PGP Public Key.
Protocol Public Keys	Defines the required parameters that you must enter to add a Protocol Public Key.
Tags	Defines the required parameters that you must enter to enter to add a tag.

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** from the **Results Table**.

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

Testing the Connectivity

You can use the **Test Connectivity** option to check the connectivity status for the server.

> **Note:** Use this option 30 seconds after adding the server.

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.

Task	Description
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 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 credential 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 credential 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 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 is displayed. You can also delete transfers from the **Manage Transfers** 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 must also 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: • 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.

Tab	Description
	• 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 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, 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.

Tab	Description
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

Tab	Description
	mode, and a REGEX to select files to scan for violations.
Four Eyes Properties	Displayed when **Transfer Direction** is either Download or Upload and the server selected for this transfer definition has a **Server Type** of **Four Eyes**. Enables Four Eyes as the transfer definition.

Note: To automatically select fields from an existing transfer, you can click **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.
4. After clicking **Add Transfer**, an info message pops up that allows you to create Tags for the transfer. After clicking the link, the following tab is displayed.

Tab	Description
Tags	Defines the parameters that are required to enter to add a tag.

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	Allows you to create a new transfer definition.

Task	Description
Site	
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.**

Platform Server Transfers

As an administrator, you can save Platform Server transfer definitions and execute Platform Server transfers. The Platform Server transfer page is only displayed on MFT Command Center. Platform Server Transfer definitions can be saved in the DB to be used by subsequent Platform transfer execution. Platform transfer definitions can be executed the following ways:

- Through a JMS request
- Through a REST call
- Through scheduler jobs

You can also execute Platform Server Transfers through the Add or Update Platform Server pages. These pages define almost all parameters supported by the Platform Server clients.

Rights

The following rights are required to view, update, and execute transfer definitions:

Right	Description
FTTransferRight	Allows you to add, view, and execute platform transfers but you cannot update platform transfers.
FTAdminRight	Allows you to view and update platform transfers but you cannot execute platform transfers.

Tasks

There are two tasks displayed for transfers:

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

Delegated Administration

Administration can be delegated to a department that is assigned platform 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 or Executing Platform Transfers

The TIBCO MFT Server allows you to add or execute a new platform transfer. The platform transfer information can be entered on this page. To add a new platform transfer,

complete the following steps.

Procedure

1. Click **Add/Execute Platform 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 Platform Server where the transfer will execute, local and remote file names, and connectivity information to the target platform server node. You also must define if the transfer is a `Send File`, `Receive File`, or `Send Command`.
Credentials and Server Properties	Allows you to override initiator and responder credentials. By default, the server credentials will be used as the initiator credentials and will be overridden if defined here. You can define responder credentials. It is better to define a user profile on the Platform Server initiator system. User profiles can be used to substitute the remote User ID and password based on the user initiating the transfer and the target node definition. Other parameters defined on this page include CRC checking, encryption, and whether SSL or TLS tunnel is used for this transfer.
Additional Transfer Properties	Defines many miscellaneous transfer properties. Whether you want to wait for the transfer to complete. Directory transfer properties Command type (if this is a **Send** command) Retry parameters Process name and user data • Data Properties Information about compression, write mode, data type, delimiters, and translation tables. • Accessibility

Tab	Description
	Scheduling information • Checkpoint Properties Defines whether checkpoint restart is enabled.
Email Notification	Defines transfer success and failure email recipients.
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, and whether the PPA executes on the Initiator (Local) or Responder (Remote).
JMS Properties	Defines JMS properties and selectors. This tab is only displayed when the server type is JMS.
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 Platform Server.
UNIX Properties	Defines UNIX file permissions when files are created on a target Platform Server for UNIX. Otherwise, this box is ignored.

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

3. You can perform one of the following actions on the **Add/Execute Platform Transfer** page
    a. Click the **Add** button on the upper-right side of the page to add the Platform Transfer definition to the database.
    b. Click the **Execute** button in the upper-right side of the page to execute the transfer on the selected Platform Server from the parameters defined on this page.

Managing Platform Transfers

The **Manage Platform Transfers** page displays the first 100 transfer records defined in the Command Center server. It also gives you the capability to search the transfer record 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 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 platform transfer definitions are displayed within the **Results** table. If you click the transfer ID of one of the entries in this table, the **Update/Execute Platform 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 Platform Transfer Information

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

Procedure

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

   The **Update/Execute Platform Transfer** page is displayed.

2. Enter the required changes.
3. You can perform one of the following actions on the **Update/Execute Platform**

Transfer page:

a. Click the **Update** button on the upper-right side of the page to update the Platform Transfer definition.

b. Click the **Execute** button in the upper-right side of the page to execute the transfer on the selected Platform Server from the parameters defined on this page.

c. Click the **Execute from Database** button in the upper-right side of the page to execute the transfer on the selected Platform Server from the parameters defined in the database.

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

Deleting a PlatformTransfer

When deleting a Platform Transfer definition, the System Configuration **Check Dependency Before Delete** parameter determines if a dependency check is performed. When enabled, prior to deleting a Platform Transfer definition, a dependency check is performed for the scheduler jobs configured to this Platform 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 Platform 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.**

Alerts

As an administrator, you can perform an action based on an event that occurred or did not occur. The Alert pages are only displayed on MFT Command Center. There are three types of alerts:

Alert	Action Performed Based On
Logon Alerts	A user logging in.
Transfer Alerts	A transfer completed, either successfully or unsuccessfully.
Non-Transfer Alerts	A transfer not completed successfully.

Up to six actions can be performed for an alert that matches the trigger criteria:

1. Send an email.
2. Execute a Java class.
3. Execute a command (locally or on a target Platform Server).
4. Send an SNMP trap.
5. Send a JMS message to a topic or queue.
6. Send a Webhook Notification/Request to a Webhook Server.

Rights

The rights required to view and update servers are:

Right	Description
AdministratorRight	Allows you to view and update alerts.
UpdateAlertRight UpdateServerRight	Allows you to view and update alerts.
ViewAlertRight ViewServerRight	Allows you to view alerts.

Tasks

There are four links displayed for alerts:

Task	Description
Add Logon Event Alert	Allows you to create a login alert definition.
Add Transfer Event Alert	Allows you to create a transfer alert definition.
Add Transfer Non-Event Alert	Allows you to create an alert for transfers that have not been executed.
Manage Alerts	Allows you to define **Search Criteria** to display only alert definitions that match the criteria. Once a list of alerts is displayed, click the **Alert Id** to display the **UpdateAlert** page. You can also delete alerts from the **Manage Alerts** page.

Delegated Administration

Administration can be delegated to alert definitions 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 either assigned to this department or can manage this department.

> **Note:** Users assigned to a department with the necessary rights can add or update alerts but cannot define the alert action: `Execute Command`.

Adding Any Alerts

The TIBCO MFT Server allows you to add new alerts. The alert information can be entered in any of the following pages: **Add Logon Event Alert**, **Add Transfer Event Alert**, and **Add Transfer Non-Event Alert**.

To add any new alert, complete the following steps in the appropriate page.

Procedure

1. For logon event alerts, click **Add Logon Event Alert**.

   For transfer event alerts, click **Add Transfer Event Alert.**

   For transfer non-event alerts, click **Add Transfer Non-Event Alert.**

2. Enter the required information described in the table below:

Tab	Description
Required Transfer Information	Defines parameters that you must configure. This includes the alert description, and whether it is enabled.
Alert Trigger Criteria	Defines the parameter values that cause an alert to be executed. **Note:** The alert trigger criteria change depending on the alert type: **Logon**, **Transfer**, **Transfer Non-Event**)
Alert Action: Email	Defines the alert action: **Send an email**.
Alert Action: SNMP Trap	Defines the alert action: **Send an SNMP Trap message**.
Alert Action: Execute Command	Defines the alert action: **Send a command**. The command can execute locally or can execute on a target Platform Server.
Alert Action: Execute java Class	Defines the alert action: **Execute a Java Class**. **Note:** The java class is typically written by the end user. The help page shows where a sample Java class is located. The sample Java class gives instructions on how to develop and compile the Java class.
Alert Action: JMS	Defines the alert action: **Send an JMS message to a Topic or Queue**.

Tab	Description
Alert Action: Webhooks	Defines the alert action: **Send a Webhook Notification/Request to a Webhook Server**.

Note: To select the fields automatically from an existing alert, you can click **Add From Existing Alert** and select the alert link.

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

Managing Alerts

The **Manage Alerts** 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 alert records displayed. You can manage alerts using the **Search Criteria**.

Search Criteria

Search Criteria allows you to selectively search the alert 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 an alert definition will be returned. When you have completed the **Search Criteria**, click the **Search** button to perform the search and create the **Results** table.

Updating Alert Information

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

Procedure

1. Click the existing **Alert Id** from the **Search Criteria**.

   The **Update Alert** page is displayed.

2. Enter the required changes.

3. Click **Update**.

Deleting an Alert

To delete an alert, complete the following steps.

Procedure

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

Four Eyes Policies

TIBCO MFT Command Centerallows you to add Four Eyes policies if **Four Eyes** is enabled.

> **Note:** To add a policy, you should define groups for approvers and recipients beforehand.

Tasks

The following table describes the two tasks defined for Four Eyes policies.

Task	Description
Add Policy	Creates a policy
Manage Policies	Lists and Manages all the policies In the Policies list, selecting **Policy Name** displays the **Update Four Eyes policy** page. You can delete policies from **Manage Policies**.

Adding Four Eyes Policies

As an administrator, you can add a new Four Eyes policy. Enter the Four Eyes policy information on the **Add Four Eyes Policies** page. To add a new Four Eyes policy, complete

the following steps.

Procedure

1. Click **Add Policy**.
2. Enter the required information as described in the following table.

Tab	Description
Required Policy Information	Defines the 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 Four Eyes Policies

The **Manage Four Eyes Policies** page displays the policies defined in the TIBCO MFT Server. You can manage policies using the **Results Table**.

Results Table

Policy records are displayed in the **Results table**. On selecting the policy name for one of the entries, the **Update Four Eyes Policy** page pops up displaying the policy information. If authorized, you can update the Policy entry from the **Update Four Eyes Policy** page.

Updating Four Eyes Policy Information

To update an existing policy information, perform the following steps:

Procedure

1. On the **Results Table**, select an existing policy name.

   The **Update Four Eyes Policy** page is displayed.
2. Enter the required changes.
3. Click **Update**.

Deleting a Four Eyes Policy

To delete a policy, complete the following steps.

Procedure

1. Select the checkbox next to the policy 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
- License 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.

Events

As an administrator, you can display information about events that have occurred. Events are created for the following requests:

- Command Center initiated Platform Server transfers.
- Scheduler jobs
- JMS initiated requests
- FileShare requests
- Mailbox requests
- Four Eyes requests

Rights

The rights required to view events are:

Right	Description
AdministratorRight	Allows you to view and delete events.
ViewAuditRight	Allows you to view events.
HelpDeskRight	Allows you to view events.
DeleteAuditRight	Allows you to delete events.

Tasks

There are two links displayed for events:

Task	Description
Search Events	Allows you to search for events.
Delete Events	Allows you to delete events.

Delegated Administration

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

Searching Events

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

Procedure

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

   Note:
   - The **Search Criteria** allows you to filter the events that are displayed. The **Results** table displays the results of your search.
   - To get detailed information about an individual event, click **Event ID**, and the **Event Detail** page is displayed.
3. When you have finished entering the information, click the **Search** button.

Viewing Event Detail Information

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

Deleting Events

To delete an event, complete the following steps.

Procedure

1. In the **Delete event records by date or by number of days** tab, enter the event record information that you want to delete, based on a date or number of days.
2. When you have finished entering the information, click the **Delete** button on the upper-right side of the page.
3. Click **OK** to the prompt.

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, and to users that have the required rights but 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.

Server Status

The following table lists the capabilities of the Server Status page.

Capability	Description
Server Status	Allows you to display whether Internet Server or Command Center can connect to monitored servers.
Host Status	Displays information about Internet Server and Command Center instances.

Server Status

As an administrator, you can display the status of monitored server definitions.

To enable monitoring, the server definition must be configured to check the server status. To enable a server for **Server Status** monitoring, go to the Add or Update Server page and

open the **Management Options** tab. Set the **Check Server Status** parameter to **Yes**. You can also select the Internet Server or Command Center instance where the **Server Status** requests should execute.

Rights

The following rights are required to view the events.

Right	Description
AdministratorRight	Allows you to view server status.
UpdateServerRight	Allows you to view server status.
ViewServerRight	Allows you to view server status.

Delegated Administration

Administration can be delegated to the following users:

- Users with the required rights not assigned to a department.
- Users that either have the required rights assigned to the server department or can manage the server department.

Monitoring Server Status

There are two options to monitor the current status of enabled server definitions.

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the server definitions. The following table lists the fields in this section.

Field	Description
Validate Server Type	Allows you to select the type of server that you want to monitor. The default is to monitor all server definitions. Servers that support server status are: AS2, FTP, HDFS, HTTP, PS, and SSH.
Refresh Interval	Defines whether you want the page automatically refreshed. By leaving this parameter blank or specifying 0, the page will not be refreshed. If you specify a numeric value other than 0, the page will be automatically refreshed after that interval expires. The interval is defined in minutes.

Results Table

This table displays the Server Status for each server monitored. This page reports on the server status information that is created by the Status Server thread. The following table lists the status colors in the **Results** table.

Status Color	Description
Green circle with check mark	Indicates the server is up and available. For a Platform Server, it also means that the server is at a level compatible with Internet Server functions and has been configured to accept Internet Server functions.
Yellow triangle with exclamation point	Displayed only for Platform Servers. Yellow means that the server is available but the server is not at a level compatible with Internet Server functions, or is not configured to accept Internet Server functions.
Red stop sign with X	Indicates the server is down. Internet Server cannot connect to the `IPName:Port` defined in the server definition.
Blue circle with question mark	Indicates server status requests have never been attempted to this server.

Enabling Server Status Monitoring

To enable a server for server status monitoring, complete the following steps.

Procedure

1. Go to the **Add or Update Server** page and open the **Management Options** tab.
2. Set the **Check Server Status** parameter to `Yes`.

   By default, all enabled server definitions with the above definition are monitored.

Note: You can also select the Internet Server or Command Center instance where the server status requests execute.

Host Status

As an administrator, you can display information about Internet Server and Command Center instances.

The following information is displayed for each Internet Server and Command Center instance.

- Current CPU usage
- Number of threads executing
- Number of transfers executing (Internet Server only)

Rights

The **AdministratorRight** is required to view host status.

Delegated Administration

Only the super administrator can view host status.

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.

Platform Server Manual Poll Criteria

Platform Server Manual Poll Criteria allows you to connect to managed Platform Servers to report on completed transfers on that Platform Server. You can select a variety of filters to limit the transfers that are returned.

To poll Platform Servers, the following conditions must be true:

- Only Command Center can poll Platform Servers.
- The server definition management **Manage Platform Server** option must be selected.
- The Command Center User must have the **FTAdminRight** right.
- The Platform Server must be configured to accept audit requests from this Command Center server.

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**.

Resubmitting Audits

As an administrator, you can view the results of recent resubmit requests. You can resubmit Platform Server transfers from the *Search Audits* page. This page allows you to view the results of all Platform Server transfers resubmitted since you have last logged on.

Rights

The rights required to view resubmitting audits are:

Right	Description
FTTransferRight	Allows you to resubmit transfers.
ViewAuditRight	Allows you to resubmit transfers.

Delegated Administration

Administration of transfers for resubmission 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 with the same department as the audit record or users that can manage the department the audit record.

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.**

Dashboard

As an administrator, you can display a variety of dashboards. The **Dashboard** page is only displayed on MFT Command Center.

The dashboards are broken up into two categories:

- Summary
- Transfer Dashboard

Summary

The **Summary** page displays the following dashboards for the entire MFT Cluster. An MFT Cluster consists of all Internet Servers and Command Centers connected to the same database. The following table lists the components in the **Summary** page.

Component	Description
Server Status	Displays a chart of the status of the monitored servers. The chart is broken up into red (server down), green (server up), and yellow (server partially up). Click the chart and a box will be displayed with the servers with the selected status. Click the three lines in the upper-right corner to perform the following tasks: • Print the chart. • Download the chart as a PDF, PNG, JPEG, or an SVG file. • Configure the dashboard refresh Interval.
Internet Transfers	Displays a chart of the Internet Transfers completed today. The chart is broken up into green (successful) and red (failed) transfers. Click the three

Component	Description
today	lines in the upper-right corner to perform the following tasks: • Print the chart. • Download the chart as a PDF, PNG, JPEG, or an SVG file. • Configure the dashboard refresh Interval.
Internet Transfers this month	Displays a chart of the Internet Transfers completed today and in the prior 30 days. The chart is broken up into green (successful) and red (failed) transfers. Click the three lines in the upper-right corner to perform the following tasks: • Print the chart. • Download the chart as a PDF, PNG, JPEG, or an SVG file.
Internet Transfers this week	Displays a chart of the Internet Transfers completed today and in the prior 6 days. The chart is broken up into green (successful) and red (failed) transfers. Click the three lines in the upper-right corner to perform the following tasks: • Print the chart. • Download the chart as a PDF, PNG, JPEG, or an SVG file.

Rights

AdministratorRight is required to view summary dashboards.

Delegated Administration

Administration can be delegated to users with the necessary rights to view the summary dashboards, whether assigned to a department or not assigned to a department.

Transfer Dashboard

The **Transfer Dashboard** page allows you to display information about completed Internet Server and Platform Server transfers. For both Internet Server transfers and Platform Server transfers, you can select the start and end dates for the dashboard.

Component	Description
Internet Server Transfers	Allows you to report the following views for completed Internet Server transfers: • All Transfers by Host • All Transfers by Protocol • Failed Transfers by Host • Failed Transfers by Protocol • Transfers by Target Server
Platform Server Transfers	Allows you to report the following views for completed Platform Server transfers: • All Platform Server Transfers • Failed Platform Server Transfers **Note:** The Platform Server dashboards are created based on audit records collected by the Command Center from Platform Servers.

Rights

AdministratorRight is required to view transfer dashboards.

Delegated Administration

Administration with the necessary rights can view the transfer dashboards, whether assigned to a department or not assigned to a department.

Alert History

As an administrator, you can display summary and detailed information about completed alerts. You can perform these functions from within the Alert History pages:

- Search Alerts
- Delete Alerts

Rights

The rights required to view alert history are:

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

Tasks

There are two links displayed for events:

Task	Description
Search Alerts	Allows you to search for completed alerts.
Delete Alerts	Allows you to delete alert records from the database.

Delegated Administration

Administration for deleting alert history records can be delegated to users with the required rights that are not assigned to a department.

Searching Alert History

As an administrator, you can search for completed alerts. There are two components of the **Search Alerts** page:

- **Search Criteria**
- **Results Table**

Search Criteria

The **Search Criteria** page allows you to define filters to the alerts that are displayed. There are a variety of filter parameters, including alert types, transaction IDs, file names, User IDs, start date, start time, end date, and end time.

Results Table

The **Results** table displays the summary information for the alerts that have been returned. After displaying summary information, you can click on the **Alert Audit Id** to display detailed information about the selected alert.

Searching for Alert History Records

To search for completed alerts, complete the following steps.

Procedure

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

Viewing Alert Detail Information

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

Deleting Alerts

As an administrator, you can delete alert records from the database. You can delete alert 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 alert records rather than using this page.

Rights

The rights required to delete alert history records are:

Right	Description
AdministratorRight	Allows you to delete alert history records.
DeleteAuditRight	Allows you to delete alert history records.

Delegated Administration

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

Deleting Alert History

To delete an alert history, complete the following steps.

Procedure

1. Click **Delete Alerts**.
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**.

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

Criteria	Description
	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**.

Database Reports

As an administrator, you can execute database reports on various database objects. The **Database Reports** page is only displayed on MFT Command Center. The following table lists reports that are supported:

Supported Report	Description
Transfer	Reports on Internet Server and Platform Server transfers. There are three sub-reports: • Transfer Report by Server • Transfer Report by Department • Transfer Report by User For each of these reports, you can enter the date range for the report and whether you want to include Internet Transfers, Platform Transfers, or both.
Exception	Reports on Internet Server and Platform Server transfer failures. There are three sub-reports: • Exception Report by Server • Exception Report by Department • Exception Report by User For each of these reports, you can enter the date range for the report and whether you want to include Internet Transfers, Platform Transfers, or both.
Users	Reports on user departments, inactive users, and user rights. There are three sub-reports: • Users Report by Department • Inactive Users Report • User Authority Report

Supported Report	Description
	The **Inactive Users Report** allows you to specify the inactive date. Users that have not logged into the system successfully since that date are considered inactive.
Alerts	Reports on alerts. There are two sub-reports: • Alert Report By Server • Alert Report by Severity For each of these reports, you can enter the date range for the report.
AS2 Reports	Reports on AS2 transfers. There are two sub-reports: • Transfer Report by AS2 Trading Partner • Exception Report by AS2 Trading Partner

Note: All of the database reports allow you to export the report to a DOC, PDF, or a PPTX file.

Rights

The rights required to view database reports are:

Right	Description
AdministratorRight	Allows you to view database reports.
ViewAuditRight	Allows you to view database reports.

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 or can manage a department. The database report will only report on transfers, users, or alerts from the departments the user can manage.

Management

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

Function	Description
Command Center Services	Allows you to configure, start, and stop Command Center Services
Protocol Keys	Allows you to define the 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.
Scheduler	Allows you to define scheduler jobs and calendars.
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.
Connection Manager nodes	Allows you to configure Connection Manager nodes.

Command Center Services

As an administrator, you can configure, start, stop, and get the status of services on MFT Command Center hosts. The Command Center Services pages are only displayed on MFT Command Center.

Rights

The rights required to view and update Command Center Services are:

Right	Description
AdministratorRight UpdateCCServiceRight	Allows you to start, stop, and get the status of Command Center Services.
ViewCCServiceRight	Allows you to get the status of Command Center Services.

Tasks

Five links are displayed for Command Center Services:

Task	Description
Collection Service	Collects transfer audit records from servers defined as Platform Servers with the **Management** option set to `Collect Platform Server History`. The Command Center Collector connects to Platform Server, retrieve Audit records, and write the audit records to the MFT database. Once Platform Server audit records are collected, you can use **Search Audits** to view the platform transfers. The Collection Service can run on multiple Command Centers in High Availability Active/Passive mode.
Scheduler Service	Scans for scheduler jobs to be executed based on the job trigger criteria. The Scheduler Service can run on multiple Command Centers in a High Availability Active/Active mode. There are separate **Scheduler Service Status** tabs for each Command Center. You must select the Command Center host on the **Scheduler Service Status** page to get the status for that Command Center instance. There are separate **Configure Scheduler Service** tabs for each Command Center. You must select the Command Center host from the **Configure Scheduler Service** page to configure that Command Center instance.

Task	Description
	Note: When the Scheduler Service is active on multiple Command Center instances, the time on these services must be synchronized to be within less than one second.
Status Service	Connects to target Servers to check if MFT is able to connect to that target server. Only servers with the server definition Management options set to **Check Server Status** are eligible for the Status Service. Servers that support Server Status are: AS2, FTP, HDFS, HTTP, Platform Server, and SSH. Once Server Status is configured, you can use the **Diagnostics Server Status** page to view Server Status for all servers. The Status Service can run on multiple Command Centers in High Availability Active/Passive mode.
JMS Service	Used to communicate with JMS servers such as EMS. Command Center uses JMS for the following functions: • Wait for incoming transfer and retrieve audit requests on JMS queues. • Write Transfer Response records to JMS queues. • Write Alert information to JMS topics or queues. • Write Platform Server End Transfer Notification messages to JMS topics. Internet Server uses JMS for the following functions: • Write data to JMS queues or read data from JMS queues. • Write Internet Server Transfer Start and End Transfer Notification messages to JMS topics. • Write Alert information to JMS topics or queues. The JMS Service can run on multiple Internet Servers and Command Centers (runs in a High Availability Active/Active mode). There are separate **JMS Service Status** tabs for each Internet Server and Command Center. You must select the Internet Server or Command Center host on the **JMS Service Status** page to get the status for that instance.

Task	Description
	There are separate **Configure JMS Service** tabs for each Internet Server and Command Center. You must select the Internet Server or Command Center host on the **Configure JMS Service** page to configure that instance. **Note:** The default information is configured on the **Server Properties** and only limited parameters can be overridden for each Internet Server or Command Center instance.
Platform Service	Allows Platform Server to send a command to the Command Center to execute a scheduler job. The Command Center Platform Server Service does not support incoming file transfers. Here is how this works: Create a scheduler job. Do not create a trigger for this job Have the Platform Server initiate a SEND COMMAND request to the Command Center. The Command name is `ExecuteJob`. The `JobName` parameter defines the name of the job. The `GroupName` parameter defines the name of the group. You can also override parameters on the job by using symbolic parameters. An example of a Platform Server command to execute a job is as follows: `ExecuteJob JobName="Send File NY",GroupName=DEFAULT,LF=SourceFileName,RF=TargetFileName.` The Platform Service can run on multiple Internet Servers and Command Centers. It can run in a High Availability Active/Active mode. There are separate **Platform Server Status** tabs for each Command Center. You must select the Command Center host on the **Platform Server Status** page to get the status for that instance. There are separate **Configure Platform Service** tabs for each Command Center. You must select the Command Center host on the **Configure Platform Service** page to configure that instance.

Delegated Administration

Administration can be delegated to users with the required rights that are not assigned to a department. Only super administrators can (users with **AdministratorRight** that are not assigned to a department), start, stop, and get the status of Command Center Services.

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 private key and can be decrypted only if you have the private key and private key passphrase associated with the private key. Public keys do not contain 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

Right	Description
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 the **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 public key • Display the public 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 System 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, perform 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 keytabs.

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 trusted certificates defined in the TIBCO MFT server. It also gives you the capability to search trusted certificates and also 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 search the trusted certificates selectively and 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. On clicking an entry's **Trusted Certificate Name** in this table, a detailed page is displayed allowing 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 its transmission. 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 private key can decrypt the data.

Data is signed with the PGP system key. Any user with 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:

The 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.

The 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 encrypts and compresses 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 decrypts and decompresses 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 private key. PGP public keys 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.

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, perform 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**.

Scheduler

As an administrator, you can define calendars, jobs, and trigger criteria for the jobs. The **Scheduler** pages are only displayed on the Command Center.

The following table lists the functions allowed for the scheduler.

Function	Description
Jobs	Allows you to add, manage, and update scheduler jobs.
Calendars	Allows you to add, manage, and update scheduler calendars.

Jobs

As an administrator, you can configure jobs to execute functions based on a variety of trigger criteria. Scheduler jobs can also be chained together to execute based on success of failure of a scheduler job. The admin help pages provide a good explanation of the various scheduler and calendar options. Scheduler jobs allow you to define and execute the following job types:

Job Type	Description
Platform Transfer	Executes a Platform Server transfer.
Internet Transfer	Executes an Internet Server transfer.
Non-Event Transfer Alert	Detects if a transfer has not occurred in a defined time.
Execute Command	Executes a command locally or on a target Platform Server
Execute Java Class	Calls a Java class
Send Email	Sends an email to one or more recipients.
Batch Job	Allows you to execute a batch. **Note:** A batch is a group of scheduler jobs
Purge DB Tables	Deletes old database records.
Purge Log Files	Deletes old log files.
Key Expiration Notification	Notify users of expired keys or certificates.
Password Expiration Notification	Notify users when their password is about to expire.
Inactive Transfer Users	Disable, delete, or warn users if not logged in for a certain period of time.

Scheduling Criteria

Scheduling Information allows you to define trigger criteria to execute jobs based on the following criteria:

Trigger	Action
Execute Now	Executes a job based on date on time.

Trigger	Action
Execute Once	
By Minute	Executes a job every x minutes.
By Hour	Executes a job every x hour.
By Day	Executes a job on selected days.
By Month	Executes a job on selected months.
By Calendar	Executes a job based on an inclusion calendar

Rights

The rights required to add, delete, list, and update scheduler jobs.

Right	Description
AdministratorRight	Allows you to create, list, and update scheduler jobs. Only users with this right can purge database tables or log files.
UpdateSchedulerRight	Allows you to create, list, and update scheduler jobs.
ViewSchedulerRight	Allows you to list and view scheduler jobs.
FTTransferRight	Allows you to execute Platform Server transfers.
Execute SchedulerJobRight	Allows an admin to execute a scheduler job by clicking the **Execute Now** button in the **Update Job** page.
TransferRight	Allows you to execute Internet Server transfers.
ViewAlertRight UpdateAlertRight	Allows you to add Transfer Non-Event jobs.

Tasks

There are three links displayed for jobs.

Task	Description
Add Job	Allows you to create a new scheduler job.
Manage Jobs	Allows you to list and manage all jobs. You can define **Search Criteria** to display only jobs that match the criteria. Once a list of jobs is displayed, you can click **Job Name** and the **Update Job** page is displayed. You can also delete scheduler jobs from the **Manage Jobs** page.
Active Jobs	Allows you to display the status of active scheduled jobs.

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. The scheduler job will be assigned to that department. Platform Server or Internet Server jobs are restricted to the departments the admin user can manage.

Adding Jobs

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

Procedure

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

Tab	Description
Required Information	Defines mandatory parameters that you must configure. This includes job names and group names, descriptions, and the job type.
Platform Transfer	Displayed when **Job Type** is set to `Platform Transfer`. This tab allows you to configure information about the platform transfer to be executed. You must select a **Platform Transfer Definition** to use and define the Command Center user that the transfer executes under. You can then override parameters from the selected transfer definition.
Internet Transfer	Displayed when **Job Type** is set to Internet Transfer. Defines the information necessary to execute an Internet Server Transfer. There are three types of Internet Server Transfers: 1. JMS: Transfer data between a JMS queue and a defined transfer definition Virtual Alias. 2. File: Transfer data between a file and a defined transfer definition Virtual Alias. 3. Virtual Alias: Transfer data between two transfer definition Virtual Aliases.
Non-Event Transfer Alert	Displayed when **Job Type** is set to `Non-Event Transfer Alert`. This tab allows you to select the alert to be configured and the number of minutes to scan for completed transfers. The rest of the information is defined in the **Transfer Non-Event Alert** page.
Execute Command	Displayed when the job type is set to Execute Command. This tab allows you to select whether the command will be executed locally or on a target Platform Server. You can set the command to execute along with the parameters to be passed to the command.
Execute Java Class	Displayed when **Job Type** is set to `Execute Java Class`. You can define the class to be executed along with the parameters to be passed to the Java class.

Tab	Description
Send Email	Displayed when **Job Type** is set to `Send Email`. This tab allows you to select the recipients, the email subject, and the email text.
Batch Job	Displayed when **Job Type** is set to `Batch Job`. The only parameter that can be set is the batch to execute. When you define jobs, you can assign one or more jobs to a batch. This job type allows you to execute all the jobs in a batch.
Purge DB Tables	Displayed when **Job Type** is set to `Purge DB` tables. This job allows you to purge records from various database tables when the records are older than a defined number of days.
Purge Log Files	Displayed when **Job Type** is set to `Purge Log Files`. This job allows you to purge log and trace files from the Internet Server and Command Center instances in this MFT cluster.
Key Expiration Notification	Displayed when **Job Type** is set to `Key Expiration Notification`. Allows you to notify users by email when public keys and system keys are about to expire.
Password Expiration Notification	Displayed when **Job Type** is set to `Password Expiration Notification`. Allows you to notify users when their password is about to expire. **Note:** This job only supports database users. LDAP users are not supported.
Inactive Transfer Users	Displayed when **Job Type** is set to `Inactive Transfer Users`. Allows you to disable, delete, or warn transfer users if not logged in for a certain period. **Note:** This job only supports database users. LDAP users are not supported.

Tab	Description
Scheduling Information	Allows you to define the job trigger information. The trigger information allows you to define the days, times, and intervals when a transfer executes.
Additional Information	Allows you to define whether the job runs exclusively and whether the job is recoverable. You can also define a dependent job that executes if this job is successful or if it fails.

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

Managing Jobs

The **Manage Jobs** page displays the first 100 job records defined. It also gives you the capability to search the job record database to limit the number of records displayed. There are two options to manage jobs:

- Search Criteria
- Results Table

Search Criteria

Search Criteria allows you to selectively search the job record database to limit the number of records that are displayed on the job results table. 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

All job records are displayed within the **Results** table. If you click the job 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 Job Information

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

Procedure

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

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

Deleting a Job

To delete a job, complete the following steps.

Procedure

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

Listing Active Jobs

The **Active Jobs** page displays the list of active jobs running in the TIBCO MFT server.

Results Table

All active jobs executing on the selected Command Center are displayed within the **Results** table.

Restriction: You cannot update or view these jobs from this page.

Calendars

As an administrator, you can create calendars that can be used by the scheduler to determine when scheduler jobs execute. The following table lists the different types of

calendars.

Type	Description
Exclusion	Defines dates where scheduler jobs should not execute. Exclusion calendars are typically used to exclude holidays from a scheduled job.
Inclusion	Defines dates where scheduler jobs should execute. Inclusion calendars are used to define particular days that a job should run. For example, you can create a calendar for quarterly or semi-annually jobs to execute.

Rights

The rights required to view and update calendars are:

Right	Description
AdministratorRight	Allows you to create, list, and update calendars.
UpdateSchedulerRight	Allows you to create, list, and update calendars.
ViewSchedulerRight	Allows you to list and view calendars.

Tasks

There are two links displayed for calendars:

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

Adding Calendars

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

Procedure

1. Click **Add Calendar**.
2. Enter the required information.

   When you click calendar dates, a list of the dates selected is displayed at the bottom of the page. You can click the **Remove** link to remove these dates from the calendar.

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

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

Managing Calendars

The **Manage Calendars** page displays the first 100 calendar records defined in the TIBCO MFT server. You can manage calendars by accessing the **Results** table.

Results Table

All calendar records are displayed within the **Results** table. If you click the calendar name of one of the entries in this table, a detailed page is displayed that allows you to update the entry.

Updating Calendar Information

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

Procedure

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

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

Deleting a Calendar

To delete a calendar, complete the following steps.

Procedure

1. Select the checkbox next to the calendar 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 • License 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.

Tab	Description
	• Log in Failure Attempts • 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

Tab	Description
	FTP client. It allows you to specify the ports to be used for data connections. It also defines rules about users adding their own 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 Mailbox Four Eyes

Using the **FileShare Mailbox Four Eyes** configuration page, you can configure the FileShare, Mailbox, and Four Eyes server. The fields on this page are organized into common sections with required fields marked by a red asterisk.

Rights

The **AdministratorRight** is required to view and update the **FileShare Mailbox Four Eyes** 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 Mailbox Four Eyes

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

1. Click **FileShare Mailbox Four Eyes > 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.

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.

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 generate an SAML SP metadata. To generate 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
- Time-based One-Time Password (TOTP) Authenticators, such as Google Authenticator or Microsoft Authenticator.

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

- Common MFA Configuration
- Manage MFT MFA Instances
- Updating MFT MFA Instance

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, TOTP 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 TOTP MFA, update the applicable TOTP MFA parameters.
4. Update the common MFA parameters applicable for all the MFA methods.
5. Click **Update** on the upper-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 TOTP MFA on the Update MFT MFA Instance page for the selected Host.
3. Click **update** on the upper-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 new authenticators. 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:

Tab	Description
Authenticator	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.
LDAP Connectivity	Defines the information necessary to connect to the LDAP server: • Host Name or URL and Port • Bind User DN and Password

<table>
<tr><th>Tab</th><th>Description</th></tr>
<tr><td></td><td>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 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</td></tr>
</table>

Tab	Description
	• Expiration Date • Visibility
Right Management	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 the right groups are located. This field is only used when the LDAP group name for 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 searches 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.
Group Management	Defines whether the LDAP group users are synced when a group is synced. To sync a group, select the **Enable** checkbox on the left and enter a group name in the **LDAP Group Name** or **Search Filter** box. **Group Management Base DN:** Defines the base in the LDAP tree where the groups are located. This field defines the default location for the LDAP Group Names.

Tab	Description
	Note: If an LDAP group name is fully qualified (contains the = sign) or enclosed in parentheses, this field is ignored for that group. **Groups:** A group name is listed only when enabled for LDAP on the **Add/Update group** page. To enable group syncing, select the checkbox to the left of **Group Name**. Then, specify either the name of the group in the Group Management Base DN or the fully qualified DN of the group. Members of this group are assigned to the MFT group.

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.

Results Table

All authenticator records are displayed within the **Results** table. If you click the **Authenticator Name**, the **Update Authenticator** 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 authenticator name to display the details page.
2. Enter the required changes.
3. Click **Update**.

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**.

Webhooks

As an administrator, you can either add and manage or display Webhook configurations. These configurations are used in Alerts or Transfer Definitions. When enabled and linked to an alert, Webhooks can be configured for Logon events, Transfer events, or Transfer Non-Event Alerts. Webhooks are also configurable for a successful or failed transfer notification.

Rights

You must have the **Administrator Right** to view and update Webhook configurations.

Tasks

Two links are displayed for Webhooks.

Task	Description
Add Webhook	Add a new webhook configuration.
Manage Webhooks	View, update, and delete a webhook configuration.

Adding Webhooks

As an Administrator, you can add a new webhook configuration. Use any of the following two methods to add a Webhook configuration.

- Creating a Webhook Configuration
- Importing an Existing Webhook Configuration

Creating a Webhook Configuration

To add a Webhook configuration, perform the following steps:

Procedure

1. Click **Add Webhooks**.
2. Enter the required webhook information as described in the following table.

Parameter	Description
Webhook Name	The name of the Webhook. This is a primary key and must be unique; it cannot be the same as other webhook configurations.
Webhook Description	The Description of the Webhook configuration.
Webhook URL	The URL of the Webhook to be notified.
HTTP Method	Can be either POST or PUT, depending on your requirement.
JSON PayLoad	The Webhook JSON Payload sent when the Webhook URL is called. Five sample JSON payloads are provided for use. The payload supports tokens that are replaced before the webhook is called.
HTTP Headers	Webhooks with HTTP headers should be entered in a `key:value` format. For multiple headers, use a comma to separate them.
Enabled	You can either enable or disable the Webhook.

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

Importing an Existing Webhook Configuration

To import the configuration from an existing Webhook, perform the following steps:

Procedure

1. Click **Add Webhooks**.
2. Click the **Add From Existing Webhook** button on the upper-right corner of the screen.

   You are redirected to a page with a list of existing Webhooks.
3. Select the name of the Webhook configuration that you want to import.

   The configuration is imported, and you are redirected to the **Add Webhooks** page.

Managing Webhooks

The Manage Webhooks page displays all the added Webhook configurations. You can either delete or update Webhook configurations.

- Updating a Webhook
- Deleting a Webhook

Updating a Webhook

To update a Webhook, perform the following steps:

Procedure

1. On the **Manage Webhooks** page, click the name of the Webhook you want to update from the **Results List**.

   You are redirected to the **Update Webhook** page.
2. On the **Update Webhook** page, edit the desired configuration parameters (except the Webhook name).
3. Click the **Update** button on the upper-right corner of the screen to update the Webhook configuration.

Deleting a Webhook

To delete a Webhook, perform the following steps:

Procedure

1. On the **Manage Webhooks** page, select the checkboxes to the left of the Webhook configurations you want to delete.
2. Click the trash icon above the **Results List**.
3. In the confirmation pop-up window, click **OK** to delete the selected webhook configurations.

Platform Server Management

As an administrator, you can configure, manage, and execute various Platform Server functions. The following table lists functions that are included in the **Platform Server Management** page:

Function	Description
Manage DNI Daemons	Add, update, delete, start, and stop pDNI templates.
Platform Server Nodes	Add, update, and display Platform Server Node definitions. You can save the nodes in a database or you can propagate the nodes to one or more Platform Servers.
Platform Server User Profiles	Add, update, and display Platform Server User Profile definitions. You can save the profiles in a database or you can propagate the profiles to one or more Platform Servers.
Platform Server Responder Profiles	Add, update, and display Platform Server Responder Profiles definitions. You can save the profiles in a database or you can propagate the profiles to one or more Platform Servers.

Managing DNI Daemons

The **Manage DNI Daemons** pages allows you to create, update, delete, start, and stop DNI templates. DNI is a feature of Platform Server for UNIX and Platform server for Windows. DNI allows you to automate sending and receiving files from target Platform Servers or Internet Servers. In order to use the Manage DNI Daemons page, you must first complete the following steps:

Procedure

1. Install, configure, and start the DNI daemon on the remote Windows or UNIX machine.
2. Configure the server definition to support DNI. On the **Add Server** or **Update Server** page, configure the following information in the Management tab:
    - Select the **Manage Platform Server** checkbox.
    - Configure the DNI Management port.
    - Configure the DNI Management User ID.
    - Configure the DNI Management password and confirm password.
3. Once the configuration is complete, when you select **Manage DNI Daemons**, a list of all configured DNI Daemons is displayed in the results table. Click the **Server Name** of one of the entries to display the **Manage DNI Daemon Templates** page.

Rights

The rights required to list, view, update, start, and stop DNI templates

Right	Description
AdministratorRight	Allows you to list, view, update, start, and stop DNI templates.
UpdateServerRight	Allows you to list, view, update, start and stop DNI templates.
ViewServerRight	Allows you to list and view DNI templates.

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. Department users can only manage DNI templates associated with servers assigned to departments that they can manage.

Manage DNI Daemons

When you click **Platform Server Management > Manage DNI Daemons**, a list of all servers are displayed. If you click a **Server Name** in the **Results** table, the **Manage DNI Daemon Templates** page is displayed for that server.

Manage DNI Daemon Templates

The **Manage DNI Daemon Templates** displays a list of DNI templates defined on that server. The results table displays summary information about the template, including the following fields:

- Template name.
- Status inactive or active.
- Action allows you to start (if status is inactive) or stop (if status is active) the template.
- Log allows you to view the DNI log files.

From the **Results** table, you can do the following:

Procedure

1. Click the **Template Name**. The **Template Data** tab is displayed and the template data is filled in the contents text box.
2. For an inactive template, click **Start**.
3. For an active template, click **Stop**.
4. To the **Manage DNI Daemon Logs** page, click **View Logs.**

In addition, the following table lists function buttons that are displayed in the **Template Data** tab along with a text box where the DNI template is defined:

Functions	Description
Add	Allows you to create a new DNI template.
Update	Allows you to update an existing DNI template.

If the template does not start when you click **Start**, then you should click **View Logs** for the server. The **Manage DNI Daemon Logs** page is displayed with a list of log files for that template. You can select the log you want to view. The log file will be downloaded to your local machine and you can use a text editor to view the log. If the template did not start, it is most likely due to an invalid parameter or if one of the directories does not exist. The log file will tell you the reason the template did not start.

If you click a template name, the template will be displayed in the text box at the end of this page and the template name is displayed in the **Template Name** to the right of the **Update** button. You can do the following from this page:

- Make changes to the template, click the **Update** button, and the template will be updated.
- Make changes to the template, enter a new **Template Name**, click the **Add** Button, and a new template will be added.
- Click **Generate Template** and the **Create DNI template** page is displayed.

Creating DNI Template

There are two ways to create DNI Templates:

1. Through the "**Template Data**" text box.
2. By clicking the **Create DNI Template** button.

   This displays the Create DNI template page.

Depending on the options defined, there are five tabs that can be configured:

Tab	Description
Required Parameters	Defines required parameters for all template types.

Tab	Description
Scheduling and Scanning	Defines when directory scanning is performed.
Platform Server Transfer parameters	Displayed when **Request Type** is `Send` or `Receive`. Defines Platform Server parameters.
FTP Transfer parameters	Displayed when **Request Type** is `Receive FTP`. Defines FTP parameters.
Miscellaneous Parameters	Defines miscellaneous and High Availability parameters.

As an administrator, you can perform the following tasks:

Function	Description
Generate Template	Validates the configured parameters, creates a template, returns to the **Manage DNI Templates** page, and inserts the template text into the **Template Data** text box. Then, define the template name and add the template by clicking the **Add** button.
Cancel	Returns to the **Manage DNI Templates** page without creating a template.
Clear DNI Templates	Clears all parameters entered on this page.

Note: Some parameters displayed on this page change depending on whether the **Request Type** is `Send`, `Receive`, or `Receive FTP`.

Platform Server Nodes

As an administrator, you can perform the following tasks:

- Add, manage, delete, and update node definitions in the MFT database.
- Add or replace, manage, and delete node definitions in target Platform Servers.

Rights

The rights required to list, view, and update Platform Server nodes are:

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

Tasks

There are two links displayed for users:

Task	Description
Add Platform Server Node	Allows you to create a new Platform Server node.
Manage Platform Server	Allows you to list and manage all Platform Servers.

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. Department users can only manage nodes for servers assigned to departments that they can manage.

Adding Platform Server Nodes

This page allows you to perform the following functions:

- To create a new Platform Server node.
- To add a Platform Server node from an existing platform node.
- To retrieve Platform Server nodes from managed Platform Servers.
- To update Platform Server node definitions on one or more Platform Servers.

Links

Links	Description
Add	Add the node to the database.
Update Server	Update the Platform Servers selected in the **Server List** tab.
Add from Existing Platform Node	Displays the **Add from Existing Platform Node** page. This page allows you to use an existing Platform Server node as a template for this node.

Procedure

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

Tab	Description
Required Node Information	Defines required parameters, including node name, description, and connectivity information.
Additional Node Information	Defines all of the Platform Server node parameters, including default encryption and compression, password validation methods, and Command Center support.
Server List	This tab displays a list of all Platform Servers where the server definition **Manage Platform Server** checkbox is selected. This tab is used when the administrator clicks the **Update Server** button. An `Update Node` request is sent to each Platform Server checked. The result of each `Update Node` request is displayed at the top of this page.

> **Note:** To automatically select fields from an existing platform node, you can click on **Add From Existing Platform Node** and select the platform node link. This allows you to select a server profile defined in the database or a server profile defined on a Platform Server.

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

Updating Server

To update an existing platform node, complete the following steps.

Procedure

1. Click **Node Name** from the **Results Table**.
2. Enter the required changes.
3. In the **Server List** tab, select the Platform Servers that you want to update.
4. Click **Update Server**.

Managing Platform Server Nodes

This page allows you to perform the following functions:

- To list Platform Server nodes from the database.
- To update a Platform Server node in the database.
- To delete a Platform Server node in the database.
- To list Platform Server nodes from managed Platform Servers.
- To delete Platform Server nodes from managed Platform Servers.
- To update Platform Server node definitions on one or more Platform Servers.

Selecting a Pre-Existing Node Definition

There are two ways to retrieve node information:

1. From the database
2. From any Platform Server

Retrieve Nodes from the database

To retrieve nodes from the database, complete the following steps.

1. Enter the **Manage Platform Nodes** page.

   The results table displays all nodes defined in the database.

Retrieve Nodes from any Platform Server

To retrieve nodes from any Platform Server, complete the following steps.

1. Enter the **Manage Platform Nodes** page.

   The results table displays all nodes defined in the database.
2. Click **Get Nodes From Server** and select a Platform Server.

   The **Results** table displays the nodes defined to that Platform Server.

Updating Platform Node

To update an existing platform node, complete the following steps.

Procedure

1. Click the node from the **Results Table**.
2. Enter the required changes.
3. To update the database nodes, click **Update**.
4. To update the Platform Servers selected in the **Server List** tab, click **Update Server**.

Platform Server User Profiles

As an administrator, you can configure and manage user profile definitions on managed Platform Servers. A managed Platform Server is when the **Server > Management** option **Manage Platform Server** checkbox is selected.

User profiles allow Platform Server users to connect to target Platform Server without knowing the credentials of the target Platform Server. It also allows users to perform file transfers without entering credentials on the command line.

The **Platform Server User Profiles** pages allow you to do the following:

- Add, manage, delete, and update user profile definitions in the MFT database.
- Add or replace, manage and delete user profile definitions in target Platform Servers.

Rights

The rights required to list, view, and update Platform Server user profiles are:

Right	Description
AdministratorRight FTAdminRight	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
Add Platform Server User Profile	Allows you to create a new platform server user profile.
Manage Platform Server User Profiles	Allows you to list and manage all platform server user profiles.

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. Department users can only manage user profiles for servers assigned to departments that they can manage.

Adding Platform Server User Profiles

As an administrator, you can add a new Platform Server user profile. The user profile information can be entered on this page.

This page allows you to perform the following functions:

- Allows you to create a new Platform Server user profile.
- Allows you to add a Platform Server user profile from an existing Platform user profile.
- Allows you to retrieve Platform Server user profiles from managed Platform Servers.
- Allows you to update Platform Server user profiles definitions on one or more Platform Servers.

Links

Links	Description
Add	Add the user profile to the database.
Update Server	Update the Platform Servers selected in the **Server List** tab.
Add from Existing Platform User Profile	Displays the **Add from Existing Platform User Profiles** page. This page allows you to use an existing Platform Server user profile as a template for this node.

Procedure

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

Tab	Description
Required Profile Information	Defines required parameters, including node name, description, initiator user ID, Responder user ID, and password.
Server List	This tab displays a list of all Platform Servers where the server definition **Manage Platform Server** checkbox is selected. This tab is used when the administrator clicks the **Update Server** button. An `Update User Profile` request is sent to each Platform Server checked. The result of each `Update User Profile` request is displayed at the top of this page.

> **Note:** To automatically select fields from an existing platform user profile, you can click on **Add From Existing Platform Node** and select the platform node link.

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

Managing Platform Server User Profiles

This page allows you to perform the following functions:

- To list Platform Server user profiles from the database.
- To update a Platform Server user profile in the database.
- To delete Platform Server user profiles in the database.
- To list Platform Server user profiles from managed Platform Servers.
- To delete Platform Server user profiles from managed Platform Servers.
- To update Platform Server user profile definitions on one or more Platform Servers.

Updating Platform User Profiles

To update an existing platform user profile, complete the following steps.

Procedure

1. Click the node from the **Results** Table.
2. Enter the required changes.
3. To update the database user profiles, click **Update**.
4. To update the User Profile on one or more Platform Servers you must do the following:
5. Select one or more servers from the **Server List** tab.
6. Click **Update Server**.

Platform Server Responder Profiles

As an administrator, you can configure and manage responder profile definitions on managed Platform Servers. A managed Platform Server is when the **Server > Management** option **Manage Platform Server** checkbox is selected.

Responder Profiles allow the Platform Server responder (that is, the server) to validate incoming requests against credentials defined by the Platform Server and not by the operating system. This means that the credentials entered by the Platform Server client does not grant access to log in to the target system. It only allows the client to perform file transfers.

The **Platform Server User Profiles** pages allow you to do the following:

- Add, manage, delete, and update responder profile definitions in the MFT database.
- Add or replace, manage and delete responder profile definitions in target Platform Servers.

Rights

The rights required to list, view, and update Platform Server user profiles are:

Right	Description
AdministratorRight FTAdminRight	Allows you to list, view, delete, and update database responder profiles records. However, you cannot retrieve or update responder 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 responder profile definitions on Platform Servers.
FTAdminRight	Allows you to list, view, delete, and update database responder profiles records.

Tasks

There are two links displayed for Platform Server user profiles:

Task	Description
Add Platform Server Responder Profile	Allows you to create a new Platform Server responder profile.
Manage Platform Server Responder Profiles	Allows you to list and manage all Platform Server responder profiles.

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. Department users can only manage responder profiles for servers assigned to departments that they can manage.

Adding Platform Server Responder Profiles

As an administrator, you can add a new Platform Server responder profile. The responder profile information can be entered on this page.

This page allows you to perform the following functions:

- Allows you to create a new Platform Server responder profile.
- Allows you to add a Platform Server responder profile from an existing Platform responder profile.
- Allows you to retrieve Platform Server responder profiles from managed Platform Servers.
- Allows you to update Platform Server responder profile definitions on one or more Platform Servers

Links

Links	Description
Add	Add the responder profile to the database.
Update Server	Update the Platform Servers selected in the **Server List** tab.
Add from Existing Platform Responder Profile	Displays the **Add from Existing Platform Responder Profiles** page. This page allows you to use an existing Platform Server responder profile as a template for this node.

Procedure

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

Tab	Description
Required Profile	Defines required parameters, including node name, description, initiator user ID, Responder user ID, and password.

Tab	Description
Information	
Server List	This tab displays a list of all Platform Servers where the server definition **Manage Platform Server** checkbox is selected. This tab is used when the administrator clicks the **Update Server** button. An `Update Responder Profile` request is sent to each Platform Server checked. The result of each `Update Responder Profile` request is displayed at the top of this page.

Note: To automatically select fields from an existing platform responder profile, you can click on **Add From Existing Profile** and select the platform node link. This allows you to select a Responder Profile defined in the database or a Responder Profile defined on a Platform Server.

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

Updating Server

To update an existing platform responder profile on one or more Platform Servers, complete the following steps.

Procedure

1. Click **Profile ID** from the **Results** Table.
2. Enter the required changes.
3. Click the **Server List** tab and select one or more Platform Servers.
4. Click **Update Server**.

Managing Platform Server Responder Profiles

This page allows you to perform the following functions:

- List Platform Server responder profiles from the database

- Update a Platform Server responder profile in the database
- Delete Platform Server responder profiles in the database
- List Platform Server responder profiles from managed Platform Servers
- Delete Platform Server responder profiles from managed Platform Servers
- Update Platform Server responder profiles definitions on one or more Platform Servers

Updating a Pre-Existing Node Definition

To select a pre-existing node definition, you can complete the following steps:

1. When you enter the **Manage Platform Server Responder Profiles** page, a list of Responder Profiles defined in the database is the **Results** table.
2. Click **Get Responder Profiles from Server.**

   A list of managed Platform Servers is displayed.
3. Select a Platform Server and a list of responder profile definitions on that Platform Server are displayed.
4. Select a responder profile from the **Platform Server Results** table.
5. To retrieve Responder Profiles from the database, click **Get Responder Profiles from Database**.
6. Select a responder profile from the **Results** table.

Updating Platform Responder Profiles

To update an existing platform responder profile, complete the following steps.

Procedure

1. Click profile from the **Results** table.
2. Enter the required changes.
3. To update the database responder profiles, click **Update**.

Updating Responder Profile on One or More Platform Servers

To update the Responder Profile on one or more Platform Servers, complete the following steps.

Procedure

1. Select one or more servers from the **Server List** tab.
2. Click **Update Server**.

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 the following functions for Transfer 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 UpdateTransferServiceRight	Allows you to get and update the status of Transfer Services.
ViewTransferServiceRight	Allows you to get the status of Transfer Services.

Tasks

The following links are displayed for Transfer Servers.

Task	Description
AS2 Server	Allows you to configure and manage the AS2 server
FTP Server	Allows you to configure and manage the FTP server
SSH Server	Allows you to configure and manage the SFTP server
OFTP2 Server	Allows you to configure and manage the OFTP2 server
Platform Server	Allows you to configure and manage Platform Server

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.

Parameter	Description
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 Message	Defines the message that is displayed when you log in to the MFT FTP 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.

Parameter	Description
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 Certificate	Defines whether keys, certificates, or both are used for incoming requests 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/Groups in These Authenticators	All users and all roles for the defined authenticators are synced. All the defined Groups that have the **LDAP Group** checkbox selected are synced.
Sync All Groups in these Authenticators	Only the Groups that have the **LDAP Group** checkbox selected are synced.

After you enter the necessary information, select **Sync**. You can either select an authenticator from the menu or select **All**.

Note: Syncing an authenticator can take a few minutes, especially when you are syncing the 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.
- For **Sync All Groups in these Authenticators**, if a user is in the LDAP Group but not in the MFT database, the user is not added to the MFT database and only the existing users are synchronized with the defined groups.

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.

Active Transfers

As an administrator, you can view active Internet Server and Platform Server transfers.

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

Link	Description
Internet Server Transfers	Allows you to view active Internet Server transfers.

Link	Description
Platform Server Transfers	Allows you to view and optionally cancel active Platform Server transfers.

Internet Server Transfers

When this page is entered, a dashboard that shows all Internet Servers with active transfer is displayed. The **Results** table shows summary information about the active transfers. If you click the **Audit Id** of an active transfer, a pop-up shows additional details of the selected transfer. You can select **Refresh** on the pop-up to track the transfer until it completes.

Rights

The rights required for **Internet Server Transfer** pages are:

Right	Description
AdministratorRight	Allows you to list and view active Internet Server transfers.
ViewAuditRight	Allows you to list and view active Internet Server transfers.

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 Server transfer functions.

Platform Server Transfers

When this page is entered, you must select **Remote Platform Server** to monitor. The list of Platform Servers in the **Remote Platform Server** box includes all Platform Server definitions where the server definition management Options: **Manage Platform Server**

checkbox is selected. Once a Platform Server is selected, Command Center polls the selected Platform Server to get a list of all active and inactive transfers executing on that Platform Server. The **Results** table shows summary information about the active transfers. If you click the **ID** of an active transfer, the **Active Platform Server Transfer Detail** page is displayed.

Active Platform Server Transfers

This page shows detailed information about the transfer executing on the selected Platform Server.

Note: Viewing Active Platform transfers requires Platform Server version 8.1.0 or higher.

The following table lists the two links displayed, depending on the user rights:

Link	Description
Refresh	Allows you to track the transfer until it completes.
Cancel Transfer	Allows you to cancel the transfer. This requires that the user have `FTAlterRight`.

Note: Cancelling Platform Transfers requires that the Platform Server node definition for this Command Center Support altering transfers.

Rights

The rights required for **Internet Server Transfer** pages are:

Right	Description
FTAdminRight	Allows you to list and view active Platform Server Transfers
FTAdminAlterRight	Allows you to list and view active Platform Server transfers. Also, gives you the ability to cancel active Platform Server transfers.

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 Platform Server transfer functions.

Hawk Microagent

Status

As an administrator, you can stop, start, and display the status of the Hawk Microagent on the Command Center and Internet Server instances.

Function Operation

The following table lists the functions that you can perform.

Function	Operation
Start	Starts the Hawk Microagent.
Stop	Stops the Hawk Microagent.
Status	Displays the Hawk Microagent status.

Configuration

As an administrator, you can configure the Hawk Microagent for the Command Center and Internet Server instances. To do so, select the server you want to configure.

Parameter Description

The following parameters can be configured for the Hawk Microagent.

Parameter	Description
Host Name	The name of the Command Center or Internet Server instance.
Enabled	Configures whether the Hawk Microagent is enabled or disabled.
Display Name	The name of the Microagent displayed on the Hawk Console.
Description	The description of the Microagent displayed on the Hawk Console.
Domain	The Hawk domain to which the Microagent belongs. For more information, see the TIBCO Hawk® documentation.
Agent Name	Typically set to **none**. For more information, see the TIBCO Hawk® documentation.
Daemon	The port number on which the Microagent listens.
Network	A specific network for outbound multicast Rendezvous communications. Leave this field clear by default. For more information, see the TIBCO Hawk® documentation.
Service	The port number on which the Microagent listens.

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 Command Center 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
- Alerts
- Audits
- Collector
- Database Reports
- Departments
- Diagnostics
- FTP Server Configuration
- Groups
- Platform Nodes
- Platform Responder Profiles
- Platform Transfers
- Platform User Profiles
- Server
- Server Credentials
- Statistics
- 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. Department administrators with UpdateSessionRight can delete and view active users in their departments.
Super Administrator	Super administrators can view or delete any active users.

Alerts

Alerts administrative tasks can be limited by the rights that are assigned (or not assigned) to a user. In addition to AdministratorRight, administrative users can also be assigned ViewAlertRight and UpdateAlertRight.

Add Alert

Role	Description
Department Administrator	Department administrators can add alerts to the system, but they are limited as to which alert actions can be taken. When department administrators add an alert, they can assign the alert to their own departments or to any departments that they can manage. By default, the alert is assigned to the departments to which the department administrators belong. Department administrators can change the department that an alert is defined for to their own departments or to the departments that they can manage.

Role	Description
Super Administrator	Super administrators can add alerts to the system utilizing any type of alert action available.

Manage Alert

Role	Description
Department Administrator	Department administrators can list, update, and delete alerts for their own departments and for the departments that they can manage.
Super Administrator	Super administrators can list, update, and delete alerts from all departments in the system.

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.

Role	Description
	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 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.

Collector

Only super administrators can perform Collector tasks.

Database Reports

Database report administrative tasks can be limited by the rights that are assigned to a user.

Role	Description
Department Administrator	To administer database reports, department administrators must have DBReportsRight. The data in the report is limited by the department of the target resource.
Super Administrator	Super administrators, with only AdministratorRight, can administer database reports. No additional rights are necessary.

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.

Role	Description
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 their departments and the **Department** parameter of a group definition assigned to any departments that they can manage.

Role	Description
	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.

Platform Nodes

Administrative tasks can be limited by the rights that are assigned (or not assigned) to a user.

Add Platform Node

Role	Description
Department Administrator	Department administrators can add a Platform node to the system, and assign the node to their own departments or any departments that they can manage. By default, the node is assigned to the departments to which the department administrators belong.
Super Administrator	Super administrators can create a Platform node which can be assigned to any department in the system or set to none. A Platform node that is not assigned to a department has no special properties.

Update Platform Node

Role	Description
Department Administrator	Department administrators can list, update, and delete Platform nodes assigned to their own departments and the departments that they can manage. Department administrators can change the department to which the Platform node is assigned to their own departments or to any departments that they can manage.
Super Administrator	Super administrators can list, update, and delete all platform nodes in the system. The department that the platform node is assigned to can be changed to any department in the system or to none.

Platform Server Responder Profiles

Platform administrative tasks can be limited by the rights that are assigned (or not assigned) to a user. In addition to AdministratorRight, administrative users can also be assigned FTAdminRight.

Add Platform Responder Profile

Role	Description
Department Administrator	Department administrators can add a Platform responder profile to the database, and assign it to their own departments or any departments that they can manage. By default, the Platform responder profile is assigned to the departments to which the department administrator belongs.
Super Administrator	Super administrators can add Platform responder profiles to any department in the system.

Update Platform Responder Profile

Role	Description
Department Administrator	Department administrators can list, update, and delete Platform responder profiles assigned to their own departments and the departments that they can manage.
Super Administrator	Super administrators can list, update, and delete any Platform responder profile in the system.

Platform Transfers

Because Platform transfers can be done on the fly, no department is assigned to an individual ad hoc transfer. However, Platform transfers created and added to the system can have a department assigned to it. When a department user enters the Manage Platform Transfers page, Platform transfers assigned to the user's department and Platform transfers assigned to the departments that this user can manage are listed.

A Platform transfer can be assigned to only one department in the system. The administrator can choose not to assign a department to the transfer, but this offers no special properties to the transfer. If a transfer is assigned to a particular department, it can only be administered by super administrators or users with FTAdminRight. Platform transfers do not have visibility associated with them. Department administrators can access or view transfers of their departments and transfers of the department that they can manage. When users with FTTransferRights log in to perform a Platform transfer, they can see all the transfers that they are authorized to access.

Role	Description
Department Administrator	Department administrators can see transfers assigned to their departments and the departments that they can manage. Department administrators can change the department to which the transfer definition is assigned to their own departments or to any departments that they can manage.

Role	Description
	Note: Pay special attention when changing the department on a transfer definition.
Super Administrator	If super administrators update a transfer definition originally created by department administrators, only the information that the department administrators have access to can be used. Otherwise, an error occurs. Super administrators can change the department to which the transfer definition is assigned to any department in the system or to none. **Note:** Pay special attention when changing the department on a transfer definition.

Add/Execute Platform Transfer

Role	Description
Department Administrator	Department administrators can define a Platform transfer, and assign it to their departments or any departments that they can manage. By default, the Platform transfer is assigned to the departments to which the department administrators belong. When selecting Initiator Platform Server, only servers assigned to this department, servers assigned to the departments that the department administrator can manage, and servers with public visibility can be used.
Super Administrator	Super administrators can define a Platform transfer, and assign it to any department in the system or to none. When selecting the Initiator Platform Server, servers assigned to any departments in the system can be used.

Manage Platform Transfers

Role	Description
Department Administrator	Department administrators can update, list, and delete any Platform transfer that is assigned to their departments and the departments that they can manage. When selecting an Initiator Platform Server, only servers assigned to this department, servers assigned to the departments that the department administrator can manage, and servers from other departments with public visibility can be used. Department administrators can change the department to which the Platform transfer is assigned to their own departments or to any department that they can manage. **Note:** Pay special attention when changing the department on a transfer definition.
Super Administrator	Super administrators can list, update, and delete any Platform transfer definition in the system. When selecting an Initiator Platform Server, servers assigned to any departments in the system can be used. Super administrators can change the department to which the Platform transfer is assigned to any department in the system or to none. **Note:** Pay special attention when changing the department on a transfer definition.

Platform User Profiles

Platform administrative tasks can be limited by the rights that are assigned (or not assigned) to a user. In addition to AdministratorRight, administrative users can also be assigned FTAdminRight.

Add Platform User Profile

Role	Description
Department Administrator	Department administrators can add a Platform user profile to the database, and assign it to their own departments or to any departments that they can manage. By default, the Platform user profile is assigned to the departments to which the department administrators belong.
Super Administrator	Super administrators can add Platform user profiles to any department in the system.

Update Platform User Profile

Role	Description
Department Administrator	Department administrators can list, update, and delete Platform user profiles assigned to their own departments and the departments that they can manage.
Super Administrator	Super administrators can list, update, and delete any Platform user profile in the system.

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.

Statistics

Only super administrators can perform these tasks.

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.

Role	Description
	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. 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.

Role	Description
	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.

Platform Server Functionality

TIBCO MFT Platform Server can be configured and managed, and transfers can be initiated through Platform Server interfaces; these interfaces require access to the actual TIBCO MFT Platform Server computer. Most functions are executed through a command line program or by editing a configuration file. Many of these functions can also be performed by TIBCO MFT Command Center. TIBCO MFT Command Center contains a single point at which many of these functions can be executed.

TIBCO MFT Command Center is installed on an embedded J2EE application server. You can log onto TIBCO MFT Command Center through a web browser to configure, manage, and perform transfers on TIBCO MFT Platform Servers.

The features that are supported by TIBCO MFT Command Center are those that are often performed more frequently after TIBCO MFT Platform Server is installed. The following table lists the supported functions.

Note: All TIBCO MFT Platform Server systems support the functions listed in the following table. The existing command line utilities remain in the system and might still be used.

Function	Description
Collector	Retrieves information on completed transfers from TIBCO MFT Platform Server systems and stores the information in a database.
Audit Polling	Allows you to dynamically inquire on completed transfers on TIBCO MFT Platform Server systems that are not utilizing the collector.
Node Configuration	Allows you to add, list, update, and delete TIBCO MFT Platform Server node entries.
User Profile Configuration	Allows you to add, list, update, and delete TIBCO MFT Platform Server user profile entries.

Function	Description
Responder Profile Configuration	Allows you to add, list, update, and delete TIBCO MFT Platform Server responder profile entries.
Executing Transfers	Allows you to perform file transfers between two TIBCO MFT Platform Server systems.

Platform Server Requirements

To perform TIBCO MFT Platform Server functions from TIBCO MFT Command Center, certain configurations must be made.

The following requirements must be fulfilled by TIBCO MFT Platform Server:

- Node Authentication
- Security Authentication
- Security Authorization

Node Authentication

TIBCO MFT Platform Server does not accept requests from any TIBCO MFT Command Center servers until they are configured to do so. TIBCO MFT Platform Server servers are required to define the actual TIBCO MFT Command Center servers from whom they will accept requests. This is done through a TIBCO MFT Platform Server node definition.

For each TIBCO MFT Command Centersystem (typically only one with a possible backup server), a node definition must be built, and the **Command Center Support** parameter must be set. This parameter supports you to define the individual functions that can be performed by TIBCO MFT Command Center. If a Platform node definition is not defined for TIBCO MFT Command Center, or if the Platform node definition does not support a particular function, the request is terminated and an error message is returned to the user. Giving TIBCO MFT Command Center the ability to perform a Platform Server function does not mean that a user can perform that function. The user must still be given the authorization to perform this function. For details on additional authentication and authorization checking, see Security Authentication and Security Authorization.

The following table defines the options available to the Platform Server Node definition **Command Center Support** parameter:

- NODE: supports TIBCO MFT Platform Server to accept TIBCO MFT Command Center requests to add, list, update, and delete TIBCO MFT Platform Server node entries.
- PROFILE: supports TIBCO MFT Platform Server to accept TIBCO MFT Command Center requests to add, list, update, and delete TIBCO MFT Platform Server user profile and responder profile entries.
- TRANSFER: supports TIBCO MFT Platform Server to accept TIBCO MFT Command Center requests to initiate a transfer on this TIBCO MFT Platform Server to send a file to a different TIBCO MFT Platform Server system.
- AUDIT: supports TIBCO MFT Platform Server to accept TIBCO MFT Command Center requests to view and retrieve information in the TIBCO MFT Platform Server audit log. TIBCO MFT Command Center Collector and Audit Polling functions require this option to be set on the TIBCO MFT Platform Server node definition.
- ALL: supports TIBCO MFT Platform Server to accept all TIBCO MFT Command Center requests. All of the functions within NODE, PROFILE, TRANSFER, and AUDIT are allowed.
- ALTER: Allows canceling Platform Transfers through the **Active Transfers > Platform Server Transfers** page. Note that ALTER is not included in ALL.
- NONE: TIBCO MFT Platform Server does not support any TIBCO MFT Command Center requests.

Security Authentication

To maintain a secure environment, TIBCO MFT Platform Server must validate that the TIBCO MFT Command Center user attempting to perform a TIBCO MFT Platform Server function is a valid user.

When a TIBCO MFT Command Center user attempts to perform a function, an encrypted user ID and password are passed from TIBCO MFT Command Center to TIBCO MFT Platform Server. TIBCO MFT Platform Server verifies that the user is valid and that the password is valid for that user ID. Only after this validation is completed successfully can the TIBCO MFT Platform Server function be continued.

Security Authorization

Authentication of a user ID and password is only half the task. TIBCO MFT Platform Server must still make sure that the user is authorized to perform the TIBCO MFT Platform Server function. After a user is authenticated, TIBCO MFT Platform Server checks whether the authenticated user is authorized to perform the particular function.

The checking mechanism used to determine whether a user is authorized for a particular function is the same as that used by the existing command line programs. The following tables list the function, and the necessary rights that must be configured to support a user to use TIBCO MFT Command Center to perform a TIBCO MFT Platform Server function on each operating system. For more detailed information on these features, see *TIBCO Managed File Transfer Platform Server User's Guide* for the individual platforms.

TIBCO MFT Platform Server for IBMi Authorization

Function	Security Validation
Audit Polling Collector	If the user has QSECOFR, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is authorized to change the following data areas: cfadmin, cfbrowse. If the user is authorized to change one of these data areas, the user is authorized to perform this function.
Execute Transfers	If the user has QSECOFR, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is authorized to change the following data areas: `cfadmin`, `cfbrowse`. If the user is authorized to change one of these data areas, the user is authorized to perform this function.
Node User Profile Responder Profile	If the user has QSECOFR, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is authorized to change the following data area: cfadmin. If the user is authorized to change this data area, the user is also authorized to perform this function.

TIBCO MFT Platform Server for UNIX Authorization

Function	Security Validation
Audit Polling Collector	If the user is a root user (or `UID=0`), the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of one of the following two UNIX groups: cfadmin, cfbrowse. If the user is a member of either group, the user is authorized to perform this function.
Execute Transfers	If the user is a root user (or `UID=0`), the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of one of the following two UNIX groups: `cfadmin`, `cftransfer`. If the user is a member of either group, the user is authorized to perform this function.
Node User Profile Responder Profile	If the user is a root user (or `UID=0`), the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of the following UNIX group: cfadmin. If the user is a member of this group, the user is authorized to perform this function.

TIBCO MFT Platform Server for Windows Authorization

Function	Security Validation
Audit Polling Collector	If the user is a Windows administrator, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of one of the following two Windows groups: cfadmin, cfbrowse. If the user is a member of either group, the user is authorized to perform this function.

Function	Security Validation
Execute Transfers	If the user is a Windows administrator, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of one of the following two Windows groups: `cfadmin`, `cftransfer`. If the user is a member of either group, the user is authorized to perform this function.
Node User Profile Responder Profile	If the user is a Windows administrator, the user is authorized to perform this function. Otherwise, TIBCO MFT Platform Server checks whether the user is a member of the following Windows group: cfadmin. If the user is a member of this group, the user is authorized to perform this function.

TIBCO MFT Platform Server for z/OS Authorization

Function	Security Validation
Audit Polling Collector	TIBCO MFT Platform Server checks two RACF (or ACF2 or Top Secret) facility classes defined in the TIBCO MFT Platform Server GLOBAL configuration: **CCC_ADMIN_FACILITY**, **CCC_BROWSE_FACILITY**. If the user has read authorization for either facility class, the user is authorized to perform this function.
Execute Transfers	TIBCO MFT Platform Server checks two RACF (or ACF2 or Top Secret) facility classes defined in the TIBCO MFT Platform Server GLOBAL configuration: **CCC_ADMIN_FACILITY**, **CCC_TRANSFER_FACILITY**. If the user has read authorization for either facility class, the user is authorized to perform this function.
Node User Profile	TIBCO MFT Platform Server checks the RACF (or ACF2 or Top Secret) facility class defined by the GLOBAL **CCC_ADMIN_**

Function	Security Validation
Responder Profile	**FACILITY** resource. If the user has read authorization for this facility class, the user is authorized to perform this function.

Configuration

To perform TIBCO MFT Platform Server functions from TIBCO MFT Command Center, you have to create server definitions and server credential definitions for TIBCO MFT Platform Server in TIBCO MFT Command Center.

For more information of server definitions and server credential definitions in TIBCO MFT Command Center, see the following introductions:

- Server Definitions
- Server Credential Definitions

TIBCO MFT Command Center Server Definitions

Before performing any TIBCO MFT Platform Server functions within TIBCO MFT Command Center, you must first define TIBCO MFT Platform Servers to TIBCO MFT Command Center.

This is done through a TIBCO MFT Command Centerserver definition. You can add a server definition through the Add Server page which can be accessed by clicking **Servers > Add Server**. You must complete the information in the Required Server Information section. Make sure that you define the **Server Type** parameter as Platform Server and set the **Server Platform** parameter to the platform that TIBCO MFT Platform Server is running on. To perform TIBCO MFT Platform Server functions for this server definition, you must select the **Manage Platform Server** box in the Management Options section. The other entries within this section are used by the Collector (see TIBCO MFT Command Center User ID and Password Rules for detailed information on these entries).

The Server Credentials section supports you to assign a default TIBCO MFT Platform Server user ID and password to be used if the user ID and password are not provided in other TIBCO MFT Command Center definitions. Take special attention about defining users with a lot of rights in this definition, because this is the default user ID and password if TIBCO

MFT Command Center does not override the requests through another definition. For more information of TIBCO MFT Platform Server user and password, see User ID and Password Rules.

TIBCO MFT Command Center Server Credential Definitions

Server credentials support you to define in a more granular fashion the user ID and password that should be used when communicating with TIBCO MFT Platform Server.

While server definitions support you to define a default TIBCO MFT Platform Server user ID and password for all TIBCO MFT Command Center users, server credentials support you to specify a TIBCO MFT Platform Server user ID and password to be used when a Platform Server request is made by a specific TIBCO MFT Command Center user.

You can create a server credential through the Add Server Credentials page which can be accessed by clicking **Servers > Server Credentials > Add Server Credentials**. You must complete the information in the Required Server Credential Information section. Wherein, the **User** parameter defines the TIBCO MFT Command Center user performing a TIBCO MFT Platform Server function, while the **Server Name** parameter defines the TIBCO MFT Command Center server entry that defines the TIBCO MFT Platform Server system. The **Remote User Id** and **Remote User Password** parameters define the encrypted user ID and password to be sent to the TIBCO MFT Platform Server system when a TIBCO MFT Command Center Platform Server function is executed.

For example, assume that the TIBCO MFT Command Center administrator creates a TIBCO MFT Command Center user definition called TechSupp and a TIBCO MFT Command Center server definition called NYMFT Platform Server1 that is configured to communicate with TIBCO MFT Platform Server. The user TechSupp now wants to communicate with the server NYMFT Platform Server1. To perform any TIBCO MFT Command Center function on this server, you need a user ID and password that is valid on the server NYMFT Platform Server1. This user ID and password are used whenever the user TechSupp performs a TIBCO MFT Command Center function that requires it to communicate with the server NYMFT Platform Server1.

In this example, you build the following server credential:

Parameter	Value
User	TechSupp
Server Name	NYMFT Platform Server1
Remote User Id	TSUSER1: the name of the user on the system NYMFT Platform Server1.
Remote Password	abc123: the password for the user TSUSER1.
Confirm Password	abc123: the same information as for the **Remote Password** parameter.

If the system NYMFT Platform Server1 defines a Windows computer, you must also define the **Remote User Windows Domain** parameter in the Windows Properties section.

After defining all the parameters, click **Add** to add the server credential information. Now, whenever the user TechSupp initiates a TIBCO MFT Command Center request that requires TIBCO MFT Command Center to communicate with the TIBCO MFT Platform Server system NYMFT Platform Server1, the encrypted user ID TSUSER1 and the password abc123 are sent to the TIBCO MFT Platform Server system NYMFT Platform Server1.

TIBCO MFT Command Center User ID and Password Rules

When TIBCO MFT Command Center communicates with TIBCO MFT Platform Server systems, it tries to obtain user ID and password credentials from certain definitions in a certain order.

The following table lists where TIBCO MFT Command Center obtains user ID and password credentials when communicating with TIBCO MFT Platform Server systems. The entries in this table are listed in the order that checking is performed. If a user ID and password are found, that user ID and password are used and no additional checking is performed.

Function	Definitions Checked for TIBCO MFT Platform Server User ID and Password
Node	The following definitions are checked:

Function	Definitions Checked for TIBCO MFT Platform Server User ID and Password
User Profile Responder Profile	• The server credential for the TIBCO MFT Command Center user for that TIBCO MFT Command Center server. • The Server Credentials section of the server definition on the Add Server page. If user ID and password are not defined in the above definitions, the request terminates with an error.
Transfer	The following definitions are checked: • The **Initiator User Id** and **Initiator Password** parameters in the Credentials and Security Properties section of a Platform transfer definition on the Add/Execute Platform Transfer page. • The server credential for the TIBCO MFT Command Center user for that TIBCO MFT Command Center server. • The Server Credentials section of the server definition. If user ID and password are not defined in the above definitions, the request terminates with an error.
Platform Server Manual Poll	The following definitions are checked: • The server credential for the TIBCO MFT Command Center user for that TIBCO MFT Command Center server. • The Server Credentials section of the server definition. If user ID and password are not defined in the above definitions, the request terminates with an error.
Collector	The following definitions are checked: • The server credential for the user Collector for that TIBCO MFT Command Center server. • The Server Credentials section of the server definition. If user ID and password are not defined in the above definitions, the request terminates with an error.

User IDs and Passwords within Platform Server Transfers

TIBCO MFT Command Center requires a user ID and password to log onto the system. TIBCO MFT Platform Server authentication requires that the TIBCO MFT Platform Server initiator and responder systems have a user ID and password to perform a transfer. Therefore, three user IDs and passwords are required to perform a transfer.

TIBCO MFT Command Center and TIBCO MFT Platform Server both have facilities to automatically generate and send the user ID and password to the remote systems. The following table describes the user IDs and passwords and explains how they can be defined.

Authentication	Description
TIBCO MFT Command Center Login	This user ID and password is input by the user when logging onto TIBCO MFT Command Center using a web browser. The command line configuration program encrypts and adds the user ID and password in the `global.xml` file.
TIBCO MFT Platform Server Initiator	This information can come from one of three places in the order as described in User ID and Password Rules: • From the Platform transfer definition. • From a server credential definition. • From the Server Credentials section in a server definition. This is the default value used for any request to this server. If the information is not defined in one of the above ways, the request terminates with an error. The best way to define the TIBCO MFT Platform Server initiator user ID and password is by defining a server credential for the user and server combination.
TIBCO MFT Platform Server Responder	When the TIBCO MFT Platform Server initiator receives a request from TIBCO MFT Command Center, it then communicates with the TIBCO MFT Platform Server responder to start the file transfer request. The responder user ID and password can come from the following places in the order as

Authentication	Description
	described in User ID and Password Rules: • From the Platform transfer definition. • From a user profile defined to the TIBCO MFT Platform Server initiator. When the transfer is initiated on the Platform Server, the Platform Server scans its user profile definitions for a match on the initiating user ID and the target node. If a match is found, the responder user ID and password defined by the user profile is used for the file transfer. • TIBCO MFT Platform Server sends a trusted user to the remote TIBCO MFT Platform Server. It is up to the remote system whether the trusted user request is accepted. TIBCO MFT Platform Server for Windows does not support trusted users, and the other platforms must be configured to accept trusted users.

Extended Features

TIBCO MFT Command Center provides several extended features such as directory transfers, email notification, file token substitution, multi-language support, LDAP support, and Admin Client Utility that can be used with TIBCO MFT Platform Server.

Admin Client Utility

Admin Client Utility is designed for the administrator to conduct administrative operations through the command line on Windows and UNIX platforms. It can be invoked from a batch file, a UNIX script, and executed in unattended mode by a job scheduler for ease of use. For more information, see *TIBCO® Managed File Transfer Command Center Utilities Guide*.

Calling Admin Client Utility from Platform Server

When a TIBCO MFT Command Center transfer is created on a computer, the database must be updated to add the transfer information so that the transfer can be made available to TIBCO MFT Command Center users.

You can run Admin Client Utility through one of the following two ways:

- By executing the utility locally. This means that the machine that runs the utility must be installed with and configured for Admin Client Utility. Likewise, the proper version of Java needed by Admin Client Utility must be downloaded for that machine.
- By executing a TIBCO MFT Platform Server request on any computer that supports TIBCO MFT Platform Server. The target TIBCO MFT Platform Server computer must be installed with and configured for Admin Client Utility before this method can be used.

  For more information on how to execute the Admin Client Utility via TIBCO MFT Platform Server transfer request, see Executing Admin Client Utility from Platform Server.

Note: For more information of how to install and configure the Admin Client Utility, see *TIBCO Managed File Transfer Command Center Command Line Utilities Guide*.

Executing Admin Client Utility from Platform Server

You can run Admin Client Utility by executing a Platform Server request on any computer that supports TIBCO MFT Platform Server.

You can call Admin Client Utility through TIBCO MFT Platform Server through the following two ways:

- By executing a TIBCO MFT Platform Server command. In this method, when a file is made available, TIBCO MFT Platform Server can send a remote command to the target TIBCO MFT Platform Server where TIBCO MFT Command Center Admin Client Utility is running. This is the most flexible method of calling Admin Client Utility. TIBCO MFT Platform Server on any computer can execute this call to any version of TIBCO MFT Platform Server that is running Admin Client Utility.
- By running a TIBCO MFT Platform Server file transfer to a remote computer. You can specify a post processing action (PPA) either locally or remotely that executes the Admin Client Utility command. The advantage of using this method is that the process of transferring the file and executing Admin Client Utility is a one-step process. Admin Client Utility can be executed either locally or remotely. But CFAdmin (the name of the Admin Client Utility batch job) must run on either the local or remote TIBCO MFT Platform Server computer. You cannot execute the utility on a different computer using this methodology.

Executing Admin Client Utility as Platform Server Command

When you execute a TIBCO MFT Platform Server remote command, Admin Client Utility must be installed and configured on the remote TIBCO MFT Platform Server computer.

To execute a remote command through TIBCO MFT Platform Server, you must make the following definitions:

- Define the transfer as a send request.
- Define the transfer type as command.
- Define the remote command to be executed.
- Configure parameters that define the remote node.

Note: Although you can enter spaces within a TIBCO MFT Command Center parameter such as the **Description** parameter; it is good practice to not have any imbedded spaces in a parameter. This is because the Java implementations differ slightly over different platforms. Imbedding spaces within a parameter might cause problems with the command line. Therefore, if you want to add a description for a file you can add it as `Description: Tax_Upload_YEAR_2005`.

For samples of the parameters that can be used to send a remote command on different platforms, see the following introductions:

- Executing Commands Using Platform Server for z/OS Batch Jobs
- Executing Commands as Part of Platform Server for UNIX Transfers

Executing TIBCO MFT Command CenterCommands Using Platform Server for z/OS Batch Jobs

You can execute TIBCO MFT Command Centercommands through the batch interface of TIBCO MFT Platform Server for z/OS.

The following example is a sample of using the batch interface to send a remote command:

```
PROCESS,SENDMFT,TRANSFER,SEND
  TRANS_TYPE=COMMAND
  EXEC="/cfcc/cfccmf.sh upload         ++
        cfn:c:\temp\testabc            ++
        sfn:/tmp/testabc.upload                ++
        d:testabc_Upload_file          ++
        nn:NYNODEMFT                           ++
        uid:acctuser"
  NODE=MFTNODE
  RUSER=*PROFILE
  TRY=1
  WAIT=YES
```

The features of the above commands are as follows:

- The PROCESS statement defines that this is a send request.
- `TRANS_TYPE=COMMAND` defines that the system is sending a command rather than a file.
- The EXEC statement defines the command that should be executed. The command in the example is meant to be executed on a UNIX system running both TIBCO MFT Platform Server and TIBCO MFT Command Center Admin Client Utility. The utility is stored in the `/cfcc` directory. The script `cfccmf.sh` is created to execute this command. As the command shows, it uses an action file template. In this case, the template is called `upload.xml`. Because it uses a template, it can use the shortcut names such as CFN (client file name) and SFN (server file name).
- The `NODE` command defines the name of the remote node. The MFTNODE node must be defined to TIBCO MFT Platform Server and enabled either at startup or through the `ENA` command for this to work properly.
- The **RUSER** parameter defines that a user profile should be used to define the remote user ID and password. Alternatively, you can enter the remote user ID (the **RUSER** parameter) and remote password (the **RPASS** parameter).
- `TRY=1` indicates that you can only try to execute the command for one time.
- `WAIT=YES` means that you should wait for the command to complete rather than for the request to be scheduled.

If a parameter is not defined in the EXEC statement, the value in the template is used. If the value is not defined in either the EXEC statement or the template, a default value is used.

> **Note:** `upload.xml` is the name of the XML file that contains the XML data for this request. You must create the `upload.xml` file from the `addfile.xml` file that is included with TIBCO MFT Command Center Admin Client Utility.

The syntax for the EXEC statement is important. Because the EXEC statement is too long to fit onto one line, continuation is used to continue the parameter from one line to another. If you use double plus signs (++) to continue the parameter from one line to another, it is important that you understand how double plus signs (++) continuation works. When you use double plus signs (++) at the end of a line, TIBCO MFT Platform Server takes the current line and appends a space to the last non-blank character, and then appends the first non-space character on the next line. That means that the TIBCO MFT Platform Server batch

interface embeds a single space between the last non-space character of the current line and the first non-space character of the next line.

The batch interface runs as a stand-alone step. It is useful to use the batch interface to call TIBCO MFT Command Centerwhen a file is created by a user application. The following typical jobs are run:

1. Create the file.
2. Execute the TIBCO MFT Command Centercommand.

If you are using TIBCO MFT Platform Server to create a file on a remote system, and then want to add the file to TIBCO MFT Command Center definitions, you can use the TIBCO MFT Platform Server script interface. The following example is a sample script job that you can run to transfer a file to a remote system, and then add the file to TIBCO MFT Command Center definitions.

```
CALL SENDMFTFILE
   IF %RC <> 0 then
       SAY SEND MFT Command Center transfer terminated with RC=%RC
       EXIT 200
      ENDIF

CALL SENDMFTCOMMAND
   IF %RC <> 0 then
       SAY SEND MFT Command Center command terminated with RC=%RC
       EXIT 201
      ENDIF

SAY MFT Command Center File and Command transferred successfully
EXIT 0

:SENDMFTFILE
   PROCESS,SENDFILE,TRANSFER,SEND
      LF=prod.testabc
      RF=/tmp/testabc.cfcc
      NODE=NYNODE
      RUSER=*PROFILE
      TRY=1
      WAIT=YES
RETURN

:SENDMFTCOMMAND
   PROCESS,SENDMFT,TRANSFER,SEND
      TRANS_TYPE=COMMAND
```

```
      EXEC="/cfcc/cfccmf.sh            ++
       download                               ++
       cfn:C:\temp\testabc             ++
       sfn:/tmp/testabc.cfcc           ++
       d:testabc_Download_file         ++
       nn:NYNODEMFT                    ++
       uid:acctuser"
      NODE=MFTNODE
      RUSER*PROFILE
      TRY=1
      WAIT=YES
RETURN
```

The first step transfers a file to the NYNODE node. If that transfer is successful, the second step sends a command to the MFTNODE node to create a TIBCO MFT Command Centerfile record. When the user *acctuser* logs onto TIBCO MFT Command Center and requests a list of files, this file is made available to the user. This is still dependent on other fields in the file record such as the **Available date**, **Expiration Date**, and **Disable Flag** fields among others.

The following information shows the processes of this task:

1. The `PROD.TESTABC` file is created on the z/OS system.
2. TIBCO MFT Platform Server transfers the `PROD.TESTABC` file to the NYNODE system as the first transfer in a TIBCO MFT Platform Server script.
3. TIBCO MFT Platform Server sends a command to the TIBCO MFT Platform Server node, MFTNODE. The MFTNODE node is configured to process TIBCO MFT Command Center commands. The EXEC statement defines the MFTNODE node to add a file record for the user *acctuser*. The file record is added for the TIBCO MFT Command Center node, NYNODEMFT.

   Note: The NYNODEMFT node and the user *acctuser* must be defined to TIBCO MFT Command Center before the above command can be executed.

4. The user *acctuser* logs onto TIBCO MFT Command Center, and requests a list of files that are available.
5. The file defined as `ClientFileName(CFN):C:\temp\testabc and Description (D): testabc_Download_file` is then listed on the user's browser.
6. The user requests that TIBCO MFT Command Center transfer the file. TIBCO MFT

Command Center transfers the `/tmp/testabc.cfcc` file from the NYNODEMFT node to the user's computer. The local file is called `c:\temp\testabc`.

Note: The user has the capability of overriding the **ClientFileName** parameter (for example, local file name) but cannot change the **Node** or **ServerFileName** parameter.

Executing TIBCO MFT Command CenterCommands as Part of Platform Server for UNIX Transfers

You can execute TIBCO MFT Command Center commands through the batch interface of TIBCO MFT Platform Server for UNIX.

The following example is a sample of using the batch interface to execute TIBCO MFT Command Center Admin Client Utility as a remote command:

```
cfsend n:MFTnode trtype:command
       rcmd="/cfcc/cfccmf.sh upload
       cfn=C=\temp\testabc sfn=/tmp/testabc.cfcc
       d=testabc_Upload nn=NYNODEMFT"
```

The command above is a single line within the UNIX command line. Alternately, you can create a TIBCO MFT Platform Server for UNIX template file with all of the above information, and process the entire request through the following command:

```
cfsend t:cfccTemplate
```

The features of the above commands are as follows:

- The `cfsend` parameter indicates that this is a send request. This parameter is required.
- `n:MFTnode` defines the remote TIBCO MFT Platform Server node that is configured to process requests. This node must be defined to CFUNIX through the `cfnode` command.
- `trtype:command` defines that a command is passed to the remote system.
- The `rcmd` parameter defines the command to be executed on the remote system. Because the **rcmd** parameter contains embedded spaces, you have to enclose the remote command in double quotation marks.

Note: Based on the configuration of the local and remote TIBCO MFT Platform Server systems, you might have to add user ID and password information to the above command.

Executing Internet Server File Transfer as a Postprocessing Action

By using postprocessing actions, you can define up to four actions to be completed by the responding server when a file transfer request is completed.

If you have TIBCO MFT Internet Server installed, you can use this function to execute an MFT Internet Server Command Line Client command as a postprocessing action (PPA). The advantage of doing this is that you can perform a file transfer and then execute for instance, a file transfer command line utility command within a single step. See *TIBCO Managed File Transfer Internet Server Command Line Utilities Guide* for more information about Internet Server Command Line Client.

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

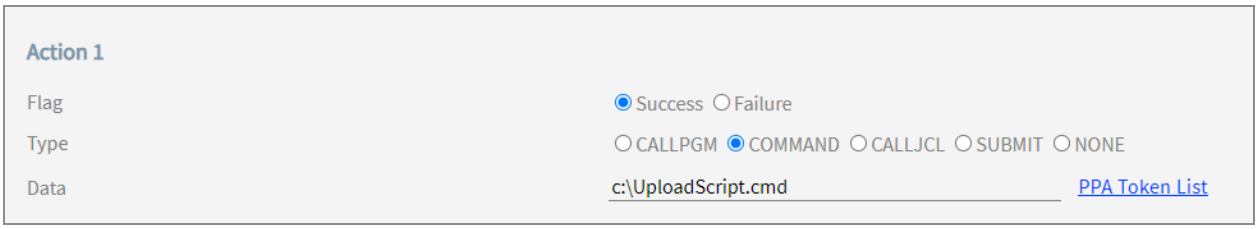
When using PPA to initiate an MFT Internet Server Command Line Client command or any command for that matter, it is good practice to get the command running successfully in batch mode first. For this example, first use the file transfer command for Internet Server Command Line Client to ensure that the 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 TIBCO MFT Internet Server, and after that file transfer request is completed, you want to launch a script that uses Internet Server Command Line Client to send that file to another MFT server.

You first make sure your Internet Server command 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 Command Center transfer definition.



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

Configuring the Target System

TIBCO MFT Command Center comes with a script that works when you issue Admin Client Utility commands. When you want to execute the Admin 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 Windows Environment
- Configuring UNIX Environment

Configuring Windows Environment

When you want to execute the Admin 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 Admin Client Utility client (CFAdmin) is installed on a Windows computer, 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\jre1.8.0_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** parameter to include the Java JRE (Java Runtime Environment). If the correct JRE is already included in the path, this step can be skipped.
- It calls the `setutilcp.bat` file included with TIBCO MFT Command Center Admin Client Utility. This file sets up environment variables needed by Java to execute.
- The last statement is the actual Java command that executes Admin Client Utility. Admin 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: Even on Windows, the Java program name (CFAdmin) is case-sensitive.

Configuring UNIX Environment

When you want to execute the Admin 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 Admin Client Utility client (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** parameter to include the JRE (Java Runtime Environment) executable files. 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 Admin Client Utility. Admin 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: The Java program name (CFAdmin) is case-sensitive.

Template Users

Five template users are added to the database during the TIBCO MFT Command Center installation process. Other users can then be added based on these templates by using the

Add From Existing User link on the Add User page. Any rights assigned to a template user are also copied to a new user.

The following table lists the template users:

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

Note: A Collector ID is also added by default. This ID is used to create server credentials for servers that also have the collection option turned on. No rights are given to this ID.

Email Processing

You can configure TIBCO MFT Command Center 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 be sent as an alert action. When certain trigger criteria are met, an email can be sent to one or several recipients. An example of such criteria can be Internet Server transfers or Platform Server transfers, transfers to or from a particular TIBCO MFT Command Centerserver, uploads, downloads, sends, receives, transfer success or transfer failure.
- Email can also be sent for Platform-to-Platform transfers. They are sent via the initiating TIBCO MFT Platform Server system and do not use the templates defined in TIBCO MFT Command Center.

TIBCO MFT Command Center email can be configured to change the look and feel so that the emails are in any format that you want. TIBCO MFT Command Center email templates are built using XML. They are simply files on the TIBCO MFT Command Center 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 Command Center provides four different email templates. For detailed information on the four email templates, see Email Templates.

To implement the email capability, you must configure the system to define when emails must be sent. For information on how to configure TIBCO MFT Command Center for email support, see Configuring TIBCO MFT Command Center for Email Support.

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

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

Configuring TIBCO MFT Command Centerfor Email Support

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

The following table lists the parameters for email support:

Parameter	Description
Email Admin User Id	This is an optional field. It defines the administrator user ID for the email server. It is only required when the email server requires a user ID and password.
Email Admin User Pwd	This is an optional field. It defines the administrator password for the email server. It is only required when the email server requires a user ID and password for authentication.
Email Failure Template	This is an optional field. It defines the default value for the **Email Failure Template** parameter. 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 is 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

Parameter	Description
	defined, the default email failure template is used: `cfcc\email-template\email-failure-template.xml`. If the template is in the TIBCO MFT Command Center`email-template` directory, you can enter the file name. Otherwise, you must enter the fully qualified file name including the path.
Email Host Name	This parameter is required if you want to use the email features. It defines the name of the email system; for example, emailserver.company.com. If this field is not defined, TIBCO MFT Command Center 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	This is an optional field. It defines the default value for the **Email Success Template** parameter. 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 is 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 is used: `cfcc\email-template\email-success-template.xml`. If the template is in the TIBCO MFT Command Center`email-template` directory, you can enter the file name. Otherwise, you must enter the fully qualified file name including the path.

Parameter	Description
SMTP TLS	This is an optional field. It defines if SSL/TLS is used for the SMTP connection. The default value is the web.xml **SmtpTLSEnabled** parameter.
Trust SMTP SSL Certificates	This is an optional field. It defines whether TLS/SSL SMTP certificates are to be trusted. The default value is No.

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 Command Centeruser 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 Command Center first looks in the TIBCO MFT Command Center server `/cfcc.war/email-template` directory for the email template file specified. If you do not specify a fully qualified name, the email templates must be stored in this default directory. If for some reason, you want to store the email template files in a different directory, you have to define the fully qualified email

template file name in the **File Notification Email Template** field.

Configuring Email Notification for File Transfer Completion

You can configure the TIBCO MFT Command Center 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** option or through the **Transfer** option.

   > **Note:** If the template is defined in both places, the TIBCO MFT Command Center Internet transfer definition overrides the TIBCO MFT Command Centersystem 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 TIBCO MFT Command Center Internet 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.

Configuring Alert Email

When an alert definition record is added to TIBCO MFT Command Center, one of the alert actions that can be taken is sending an email.

Before sending an email, TIBCO MFT Command Center checks the alert trigger criteria defined through the **Transfers > Alert** option. The alert trigger can be transfer type, server name, file name, user ID, transfer direction, and so on. You can enable alert email by selecting the **Send Email** checkbox and entering the recipient email address in the alert definition. Multiple email addresses can be defined (separated by commas).

For more information on alert definition, see Alerts.

Email Templates

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

TIBCO MFT Command Center provides the following email templates:

- File Availability Template
- Transfer Completion Templates
- Alert Template

The three 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 types of templates 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 Command Center provides a file availability template. The template is named as `email-notification-template.xml` and is located by default in the TIBCO MFT Command Center`<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 Command Centersoftware:

```
<?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 does not work.
`<sender>` `<address><token name="emailsender"/></address>`	This line defines the name of the email sender. The default sender name is cfcc@companyname.com. This name can be changed to any appropriate email address. When the user receives an email, the data entered here is 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 is shown in the Subject field of the email.

Line	Description

`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 is 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 is made available to transfer. When you click the URL, you are brought 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 Command Center 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`	These fields define the URL that can be used to

Line	Description
`following URL:` `<token name="emailurl"/>/bclient/index.jsp`	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 Command Centerfile transfer applet. **Note:** The administrators must change the field `host:port` to point to their TIBCO MFT Command Center 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 Command Center.

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 is just made available.

Token	Description
`clientfilename`	This token defines the name that is defined for the file on the client side.
`serverfilename`	This token defines the name that is defined for the file on the server side. This information is not usually displayed on the user's screen. If the notification message is sent to a user, it is good practice to not add this field to the file availability template. If this email is sent to an internal user, you can include this token in the email.
`description`	This token defines the description that is 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 on which the file will be made available to transfer.
`expirationdate`	This token defines the date on which the file will expire and be no longer valid for transfer.
`transferdirection`	This token defines whether the transfer is an upload (client to TIBCO MFT Command Centerserver) or a download (TIBCO MFT Command Center server to client).

Transfer Completion Templates

TIBCO MFT Command Center 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 TIBCO MFT Command Center`<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 transfer-notification-email SYSTEM "transfer-notification-
email.dtd">

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

<transfer-notification-email>
       <sender>
              <address><token name="emailsender"/></address>
       </sender>
       <recipient>
              <address><token name="recipientemailaddress"/></address>
       </recipient>
       <subject>File Transfer Success Notification</subject>
       <message>
              File Transferred Successfully!!
              User: <token name="userid"/>
              Transfer Description: <token name="description"/>
              Transfer Direction: <token name="transferdirection"/>
              Client File Name: <token name="clientfilename"/>
              To Server: <token name="node"/>
              Server File Name: <token name="serverfilename"/>
              Start Time: <token name="starttime"/>
              End Time: <token name="endtime"/>
              Byte Count: <token name="bytecount"/>
              Transfer Status: <token name="transferstatusmsg"/>
              Audit ID: <token name="auditid"/>
              Client IP: <token name="clientip"/>

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

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

Line	Description
`<!DOCTYPE transfer-notification-email SYSTEM "transfer-notification-`	This line defines the DTD file associated with the XML file.

Line	Description
`email.dtd">`	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 does not work.

`<sender>`
`<address><token`
`name="emailsender"/></address>`
	This line defines the name of the email sender.
	The default sender email address used is defined in the **Sender Email Address** field in the Global Settings section on the System Configuration page.
	This email address can be changed to any appropriate email address. When the user receives an email from TIBCO MFT Command Center, the data entered here is 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 receives 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`

Line	Description
	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 TIBCO Technical Support user in your company. To do this, set the user ID in the `transfer-failure-email-template.xml` file. That way, an email is sent to that user when any requests fail.
`<subject>File Transfer Success Notification</subject>`	This line defines the information that is shown in the Subject field of the email. In this case, it indicates that the file is 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="userid"/>`
`Transfer Description: <token name="description"/>`
`Transfer Direction: <token name="transferdirection"/>`
`Client File Name: <token name="clientfilename"/>`
`To Server: <token name="node"/>`
`Server File Name: <token`
	These fields define information from the definition record of the file that is transferred.
	When a token is included in the field, the information from the transfer definition and audit records is substituted for the token.

Line	Description
name="serverfilename"/> Start Time: <token name="starttime"/> End Time: <token name="endtime"/> Byte Count: <token name="bytecount"/> Transfer Status: <token name="transferstatusmsg"/> Audit ID: <token name="auditid"/> Client IP: <token name="clientip"/>	

Tokens Supported in Transfer Completion Templates

You can use tokens in the transfer completion template provided by TIBCO MFT Command Center.

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 is transferred. If done correctly, you can branch directly to the audit record for this file transfer request. It is more likely that this is included on the failure template than the success template.
`bytecount`	This token defines the number of bytes that are 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 are

Token	Description
	transferred; it defines the number of bytes that are sent or received before an error is detected.
`clientfilename`	This token defines the name that is defined for the file on the client side.
`endtime`	This token defines the time when the file transfer request is completed.
`fileid`	This token is typically used in the URL to define the record ID of the file that is transferred.
`node`	This token defines the target server associated with the file transfer.
`proxystatusmsg`	This token defines the last error message associated with the file transfer request. This is usually a better indication of the actual reason that caused a file transfer failure.
`serverfilename`	This token defines the name that is 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 is started.
`transferdirection`	This token defines whether the transfer is an upload (client to server) or a download (server to client).
`transferstatus`	This token defines the transfer status.

Token	Description
	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 fails.
`userid`	This token defines the user ID associated with the file transfer.

Alert Template

TIBCO® Managed File Transfer Command Center provides an alert template. The template is named as `email-alert-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 alert template that is shipped with the software:

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

<!-- Sample file notification template  -->

<alert-notification-email>
       <sender>
              <address><token name="emailsender"/></address>
       </sender>
       <subject>Email Alert</subject>
       <message>
              A transfer matches alert definition, and triggers the alert
processing.

              --- Alert Properties ---
              Alert ID: <token name="alertname"/>
              Alert Time: <token name="alerttime"/>
              Alert Description: <token name="alertdescription"/>
              Alert Severity: <token name="severity"/>
```

```
                --- Transfer Properties ---
                Audit ID: <token name="auditid"/>
                Department: <token name="department"/>
                File Description: <token name="description"/>
                Local Transaction Id: <token name="localTranId"/>
                Transfer Direction: <token name="transferdirection"/>
                Client File Name: <token name="clientfilename"/>
                To Server: <token name="node"/>
                Server File Name: <token name="serverfilename"/>
                Byte Count: <token name="bytecount"/>
                Start Time: <token name="starttime"/>
                End Time: <token name="endtime"/>
                Transfer Status Message ID: <token name="transferstatusmsg"/>
                Transfer User: <token name="userid"/>
                Transfer status: <token name="transferstatus"/>
                Client IP: <token name="clientip"/>
                Proxy Msg: <token name="proxystatusmsg"/>
                ProcessName: <token name="processname" />
                UserData: <token name="userdata" />

                Email comment: <token name="comment"/>

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

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

Line	Description
`<!DOCTYPE alert-notification-email SYSTEM "alert-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 does not work.
`<sender> <address><token name="emailsender"/></address>`	This line defines the name of the email sender. The default sender name is

Line	Description
	cfcc@companyname.com. This name can be changed to any appropriate email address. When the user receives an email, the data entered here is shown as the Sender (or From).
`<subject> Email Alert</subject>`	This line defines the information that is shown in the Subject field of the email. In this case, it indicates that the file is successfully transferred.
`A transfer matches alert definition, and triggers the alert processing.`	This is a comment that indicates the file is transferred successfully. You can also insert other comments or instructions here.

`Audit ID: <token name="auditid"/>`
`Department: <token name="department"/>`
`File Description: <token name="description"/>`
`Local Transaction Id: <token name="localTranId"/>`
`Transfer Direction: <token name="transferdirection"/>`
`Client File Name: <token name="clientfilename"/>`
`To Server: <token name="node"/>`
`Server File Name: <token name="serverfilename"/>`
`Byte Count: <token name="bytecount"/>`
`Start Time: <token name="starttime"/>`
`End Time: <token name="endtime"/>`
`Transfer Status Message ID: <token name="transferstatusmsg"/>`
	These fields define information regarding the transfer that triggers the alert.
	
	When a token is included in the field, the information from the transfer definition and audit records is substituted for the token.

Line	Description

`Transfer User: <token name="userid"/>`
`Transfer status: <token name="transferstatus"/>`
`Client IP: <token name="clientip"/>`
`Proxy Msg: <token name="proxystatusmsg"/>`
`ProcessName: <token name="processname" />`
`UserData: <token name="userdata" />`
 	
`Email comment: <token name="comment"/>`	

Tokens Supported in the Alert Template

You can use tokens in the file availability template provided by TIBCO MFT Command Center .

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 alert template:

Token	Description
`alertname`	This token defines the alert ID that is automatically assigned when an alert is defined.
`alerttime`	This token defines the time and date on which the alert is processed.
`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 is transferred. If done correctly, you can branch directly to the audit record for this file

Token	Description
	transfer request. It is more likely that this is included on the failure template than the success template.
`bytecount`	This token defines the number of bytes that are 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 are sent or received before an error is detected.
`clientfilename`	This token defines the name that is defined for the file on the client side.
`endtime`	This token defines the time when the file transfer request is completed.
`fileid`	This token is typically used in the URL to define the record ID of the file that is transferred.
`node`	This token defines the target server associated with the file transfer.
`proxystatusmsg`	This token defines the last error message associated with the file transfer request. This is usually a better indication of the actual reason that causes a file transfer failure.
`serverfilename`	This token defines the name that is 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.

Token	Description
	This is for information purposes only.
`starttime`	This token defines the time when the file transfer request is started.
`transferdirection`	This token defines whether the transfer is an upload (client to TIBCO MFT Command Center server) or a download (TIBCO MFT Command Center 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 fails.
`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 are 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 the **File Token List** link next to the **Server File Name** field on the Add Transfer page for the complete token list.

Multi-Language Support

TIBCO MFT Command Center supports multiple languages for various file transfer clients of TIBCO MFT Command Center . This feature supports text on the pages and 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 Command Center as follows:

- All messages and texts that are displayed to the end user using the MFT file transfer pages are displayed in the language preferred by that end user. The TIBCO MFT Command Center Administrator 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 dates and times in the TIBCO MFT Command Center Administrator pages are displayed in the U.S. format only.
- File transfer end user messages consist of texts produced by the following TIBCO MFT Command Center components:
    - File transfer web pages.
    - 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 their preferred language to TIBCO MFT Command Center 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 Command Center , all messages and texts are in English.
- TIBCO MFT Command Center supports the following languages: English, French,

Italian, and Spanish.

- Multi-language support is performed on the machine that produces the texts to be translated. In other words, language translation for JSPs and Servlets occurs on the TIBCO MFT Command Center server, while language translation for applets and File Transfer Utility occurs on the client machine.

Updating the Database Settings

You can use the `dbsettings` utility to create a new user ID and password to be used to connect to the CFCC database.

The `dbsettings` utility supports you to update the `DBUser` and `DBPass` fields defined in the `web.xml` file of your web server. The utility saves the DB password in an encrypted format if desired.

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

The following example shows a sample output:

```
* 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:\MFT711\server\webapps\mftcc\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_71
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_71
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])
```

When you change the user ID, you should choose option 4 to change the password for that user ID. You can 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 Command Center . 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 Command Center . • ManageServerRequestIS: returns the name of all Internet Server servers defined to TIBCO MFT Command Center .
`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 Command Center .

XML Schema File	Description
`ManageTransferResponseIS.xsd`	Defines the XML data that is returned when a management request is initiated, the request type is ManageTransferRequestIS and the request JMS type is ManageTransferRequestIS. This response returns 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.

XML Schema File	Description
	• Audit response: this is written when a request is accepted and the `TransferStatusCheck` parameter is set to Yes.
`TransferRequestPlatformServer.xsd`	Defines the format of the parameters required to initiate a Platform Server transfer. This is occasionally called a third-party transfer. TIBCO MFT Command Center 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 Command Center 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 Command Center 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.
`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.

Parameter	Default	Description
		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 `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,

Parameter	Default	Description
		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.
`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.

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 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.

Parameter	Default	Description
		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 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

Parameter	Default	Description
		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 processed.
`AS2TempDirectory`	No default	Defines the AS2 temporary directory. This parameter is generally defined only when very large (larger than 500 MB) AS2 files are transferred. This parameter defines MFT to use two-stage AS2

Parameter	Default	Description
		transfers. For uploads to MFT, encrypted AS2 data is written to this directory before being transferred to the target internal MFT servers. For downloads from MFT, encrypted AS2 data is written to this directory before being transferred to the target AS2 server. When this parameter is not defined, data is streamed from AS2 to the target server without writing it to a disk.
`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 authentication by these users are not attempted.
`DisplayFTPBanner`	YES	Defines whether the FTP/SFTP banner is displayed when the

Parameter	Default	Description
		user logs in. Valid values are: YES: Indicates that the FTP/SFTP banner is displayed when the user logs in. NO: Indicates that the FTP/SFTP banner is not displayed when the user logs in.
`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 instance. If defined, this parameter overrides the Systems Configuration: Global FTP Settings "Number of Ports to Use" parameter value.

Parameter	Default	Description
		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.
LDAPConnectionTimeout	20000	If MFT cannot establish a connection with the LDAP server within a certain timeout period, it aborts the connection attempt. By default, this timeout period is the network (TCP) timeout value, which is in the order of a few minutes. To change the timeout period, we can use

Parameter	Default	Description
		this parameter. The default value 20000 here means 20 seconds.
`LDAPReadTimeout`	20000	When an LDAP request is made by MFT to an LDAP server and the server does not respond for some reason, MFT waits forever for the server to respond until the TCP timeouts. On the MFT's client-side, what the user experiences are essentially a process be unresponsive. To control the LDAP request on time, a read timeout can be configured using this parameter. The default value 20000 here means 20 seconds.
`MaxConnectionCnt`	800 connections	Defines how many TCP connections are processed by each MFT protocol. This parameter applies to incoming FTP/FTPS, SSH, and Platform

Parameter	Default	Description
		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 for FTP/FTPS connections.
`MaxConnectionCntSSH`		Defines how many TCP connections are

Parameter	Default	Description
		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. There are many additional OFTP2 configuration parameters that are not defined in this tab. The web.xml parameter `OFTP2CfgFile` points

Parameter	Default	Description
		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 comma. When these users' log in, ReCaptcha is still displayed on the login page, but MFT does not perform ReCaptcha verification. This parameter only

Parameter	Default	Description
		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 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.

Parameter	Default	Description
`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 `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

Parameter	Default	Description
		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.
SocketConnectTimeout	30	Defines the socket connection timeout in seconds. Changing the value changes the time that it takes for a Platform Server, SSH, or FTP transfer to fail.
TCPBufSize	1024000	Defines the TCP buffer size used by SSH, FTP, and Platform Server connections. Using a high value increases performance over connections with high latency.

Parameter	Default	Description
`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_2	Defines the protocols supported by FTP, OFTP2, AS2 outgoing, and Platform Server SSL connections. When specifying TLSV1_3, check whether the TLSProtocolsFTPS is affecting the FTP TLS connection.

Parameter	Default	Description
TLSProtocolsPS	Values defined in TLSProtocols.	Defines the supported protocols for communicating with Platform Server using TLS connections.
TLSProtocolsFTPS	Values defined in TLSProtocols.	Defines the supported protocols for communicating with FTP using TLS connections. When specifying TLSv1_3, check the FTPSSLSessionResumption limitations for using TLSv1_3 for FTP TLS connection.
TLSProtocolsOFTP2	Values defined in TLSProtocols.	Defines the supported protocols for communicating with OFTP2 using TLS connections.
TLSProtocolsAS2Client	Values defined in TLSProtocols.	Defines the supported protocols for communicating to an AS2 server using TLS connections.
FTPSSLSessionResumption	false	Defines whether the session resumption is being used during TLS communication. When the MFT FTP

Parameter	Default	Description
		Client or Server uses TLSV1_3 and requires session resumption, set this to true.
`TLSSecurityProvider`	The default MFT security provider	Defines the security provider used by FTP and Platform Server SSL connections.
`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 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

Parameter	Default	Description
		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 the 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 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.
`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

Parameter	Default	Description
		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 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

Parameter	Default	Description
		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.
`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

Parameter	Default	Description
		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. 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.
DBPass	The encrypted database	Defines the password of the database user associated with the JDBC connection.

Parameter	Default	Description
	password defined during installation	
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.
DBType	No default	Defines the database type. This value should not be changed unless directed to by TIBCO MFT Support.
DBUser	The database user defined during installation	Defines the database user associated with the JDBC connection.
OracleDatabaseSSLCipherSuites	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA SSL_DH_anon_WITH_RC4_128_MD5 SSL_RSA_WITH_3DES_EDE_CBC_SHA	Defines the cipher suites used by Oracle JDBC connections. Different Oracle server releases require different SSL cipher suites.

Database Pooling Parameters

DB pooling parameters are used to configure database pooling.

The following table lists the DB pooling parameters:

Parameter	Default	Description
`DataBasePoolingFlag`	APACHE	Defines whether connection pooling is supported. APACHE: Indicates that connection pooling is used. None: Indicates that connection pooling is not used.
`MaxActive`	400	Defines the maximum number of active connections available to database pooling. 400 active connections should be sufficient for all but the most active MFT system.
`MaxIdle`	20	Defines the maximum number of idle connections that 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.

Parameter	Default	Description
		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.
`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

Parameter	Default	Description
		removeAbandonedTimeout.
`removeAbandonedTimeout`	60	Defines the timeout in seconds before an abandoned connection can be removed.
`logAbandoned`	false	Defines whether to log stack traces for an application code which abandoned a statement or connection. (This parameter is used for debugging purposes only) In order to see logging of abandoned connections you must set logAbandoned to true in the `web.xml` and add the following line at the end of the logging.properties file in the server/conf directory. org.apache. `tomcat.jdbc.pool.level = ALL` It should show up in the console or in the `catalina.log` file

Miscellaneous Parameters

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

The following table lists the miscellaneous parameters:

Parameter	Default	Description
`AlertCheckInterval`	60	Defines the interval in seconds between checks to see if the Alert Cache needs to be updated. Valid values are from 1

Parameter	Default	Description
		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 from 1 to 60 seconds	Defines the amount of time that Internet and Command Center waits at startup time before monitoring for cache updates and inactive hosts.
CacheTimeStampIntervalSec	30 seconds	Defines how frequently the Internet Server and Command Center

Parameter	Default	Description
		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_TEMPLATENAME environment variable.

Parameter	Default	Description
		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 that the default transfer client is the browser client. It is good practice to use the browser client by default. The value of FileShare indicates that the default transfer client is the FileShare client.
`EmbeddedServer`	true	This parameter should always be set to true.
`EscapePPATokenCharacters`	;|&	Special characters to check when the `execute PPA` command is using `EXECCMD`.
`ExpiredFilesLog`	./ExpiredFilesLog.txt	This parameter is not used.
`HostName`	The host name defined during installation	Defines the host name that is set during the

Parameter	Default	Description
		configuration process. This parameter is used to identify the MFT server in the database tables. This should not be changed without guidance from TIBCO Technical Support.
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 records that can be collected from a Platform Server on a collection request. The valid value for this parameter is a numeric value from 50 to 500.
MessageDir	The directory defined during installation	Defines the directory where MFT message

Parameter	Default	Description
		files are located.
ProtectPPATokens	Escape	Defines the action to take if you find special characters in the PPA command using EXECCMD. The values are: Reject, Escape, and Ignore.
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. **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.

Parameter	Default	Description
		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:nameid-format:transient	Allows you to update 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.

Parameter	Default	Description
SharePointTempDirectory	<MFT-Install>/server/webapps/cfcc/WEB-INF/sharepoint	Allows you to override the directory where temporary encrypted sharepoint files are written.
ServiceInactivityThreshold	5 minutes	Defines the Collector and ServerStatus inactivity timeout (in minutes). Active Collector and Server Status threads update a heartbeat every minute. When the heartbeat has not been updated for the number of minutes defined by this parameter, the service is deemed to be inactive. Passive Collector and ServerStatus thread then compete to become the active Collector or Server Status. Valid values are from 5 to 60 minutes.
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

Parameter	Default	Description
		Audits page is first configured. The value of true indicates that MFT performs an audit search when the Search Audits page is first configured. The value of false indicates that MFT does not perform an audit search when the Search Audits page is first configured. Searches 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

Parameter	Default	Description
		trusted certificates to the FTPS client.
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 bypasses the statistics update for this interval.
SyncLdapAtLogon	true	Defines whether an LDAP user is synchronized with the LDAP authenticator when HTTP users log in. The value of True indicates that LDAP users are synchronized when the user logs in. The value of False indicates that LDAP users are not synchronized with the LDAP authenticator when the user logs in. The synchronization is performed when the on-demand or scheduled synchronization occurs.

Parameter	Default	Description
`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 limits the number of concurrent JMS transfers initiated to the defined value.
`ValidationQueryTimeout`	1	Defines the number of seconds that MFT waits for a DB Pooling validation query. If the query does not return in the defined number of seconds, the connection is closed and a new connection is created.
`WebAdminLogFile`	The directory defined during installation	Defines the directory where MFT WebAdmin files are located.
`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.

Parameter	Default	Description
`reuseJMSConnection`	True for EMS implementation; False for others.	Valid values are: • True: Reuses JMS connections. • False: Creates a JMS connection for each request.
`tilesDefinitions`	`/WEB-INF/tiles.xml`	This parameter must not be changed.
`RestrictUserIdCharacters`	`%_^{}`	Disallows SQL wildcard characters in the user ID when adding a user.
`RestrictServerNameCharacters`	`%[]^{}`	Disallows SQL wildcard characters in the server name when adding a server.

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

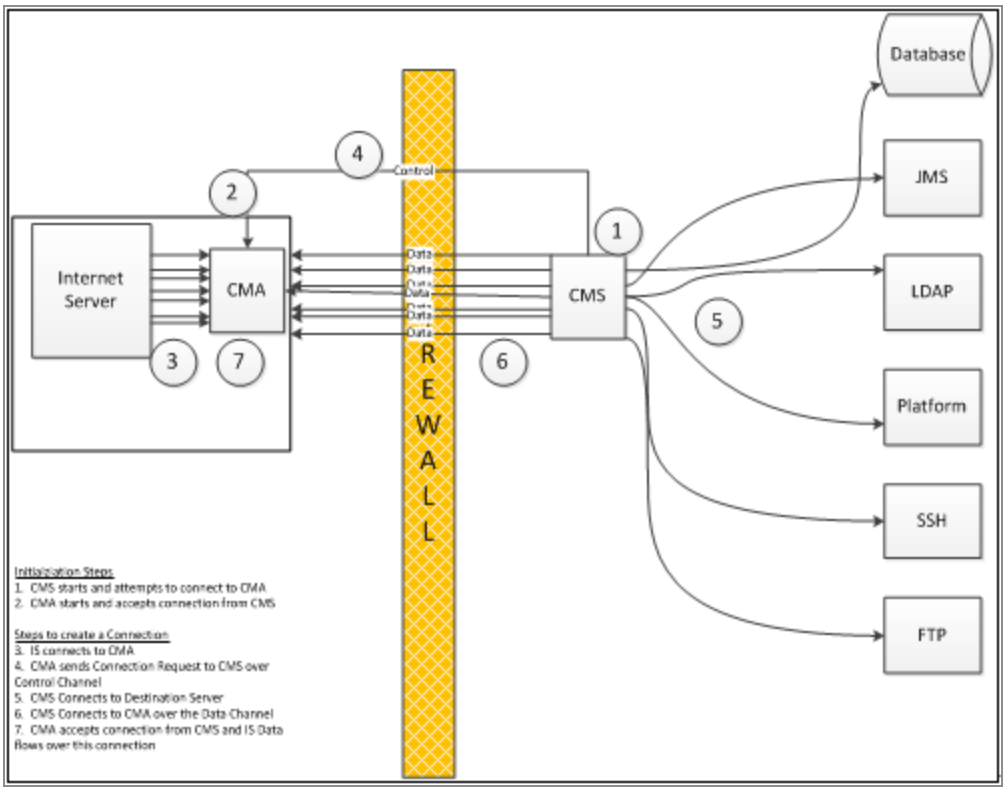
Connection Manager provides the following components: Connection Manager Agent (CMA), Connection Manager Server (CMS), , and TIBCO MFT Internet Server.

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.

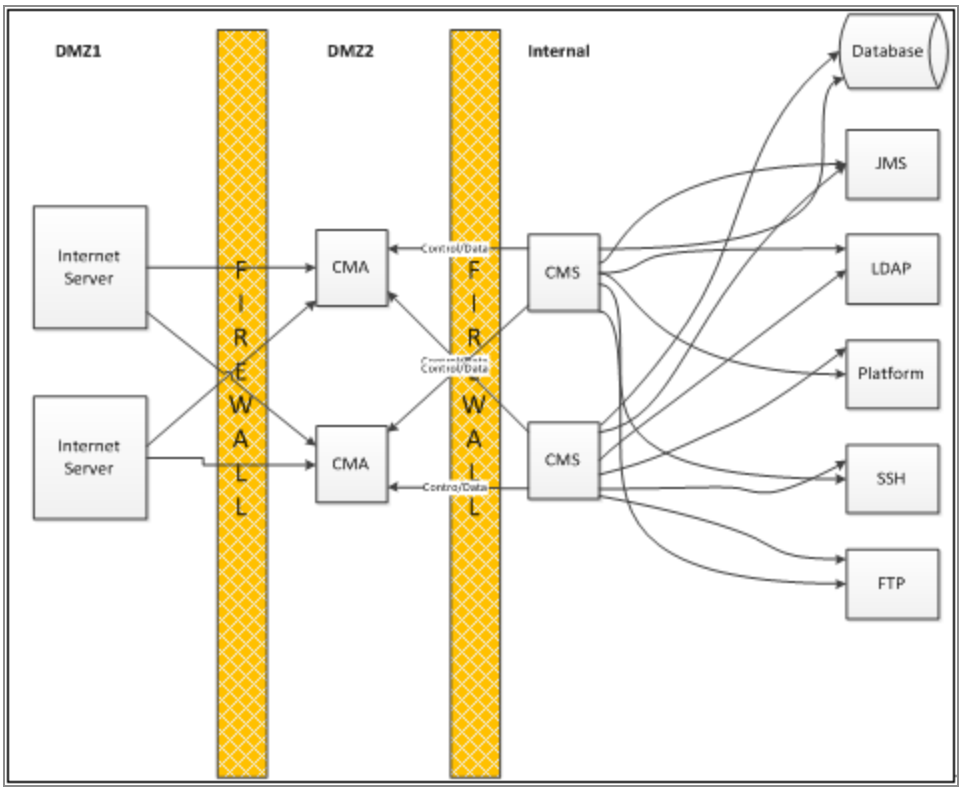
Steps to Create a Connection:

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.

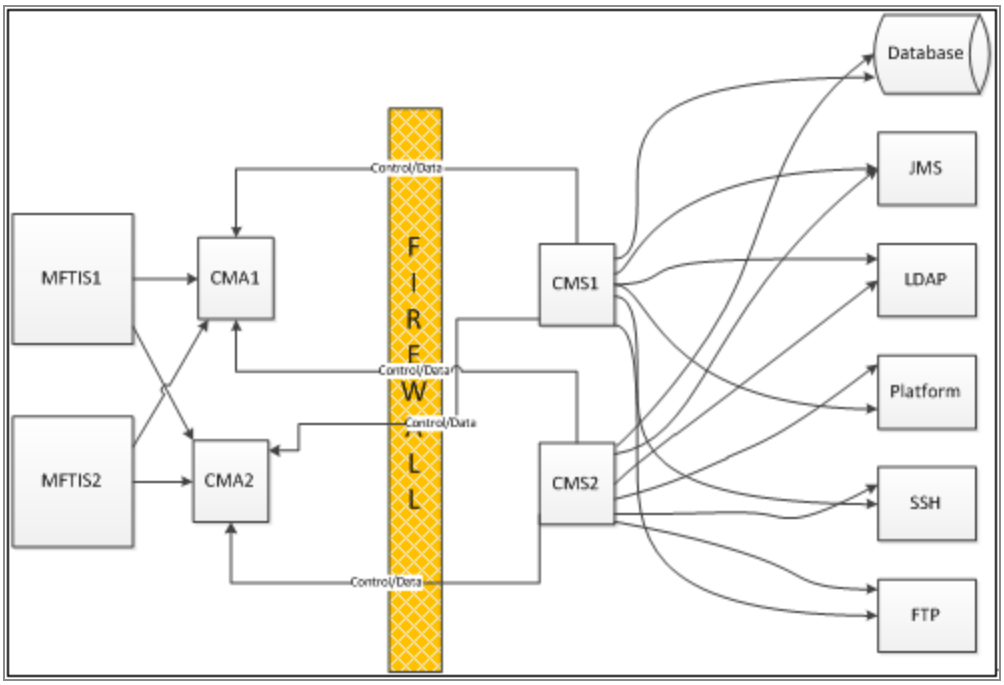
When connecting to internal servers that require many connections (for example, Internet Server connections to Oracle DB), it is best practice to minimize the number of connections established. Use of MFT Connection Pooling can minimize the number of TCP connections created between Internet Server and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

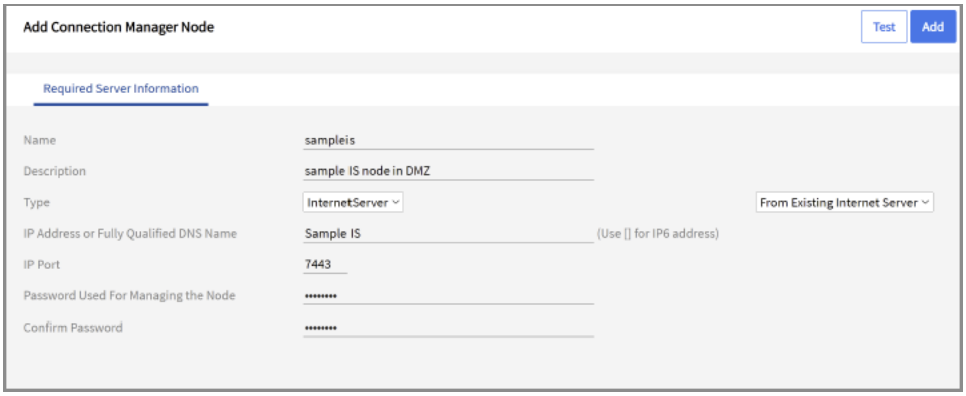
On this page, you can define the connectivity information required to communicate with the Connection Manager component.

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.

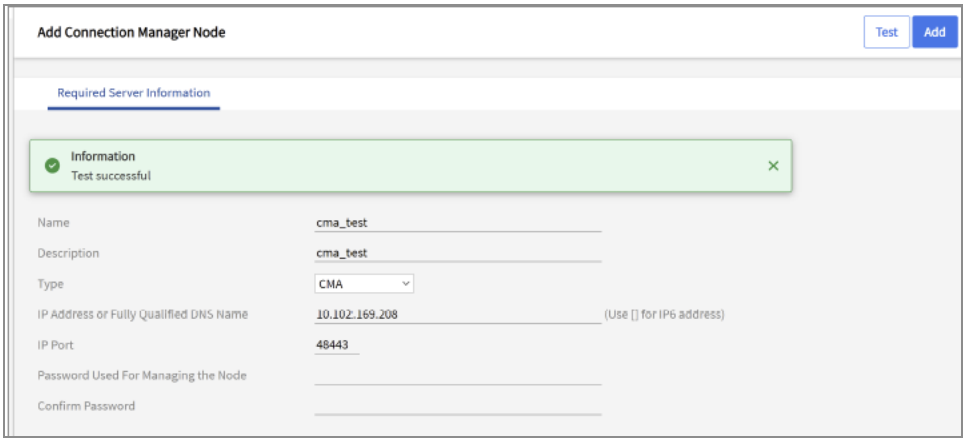
Add Connection Manager Node: Internet Server



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.

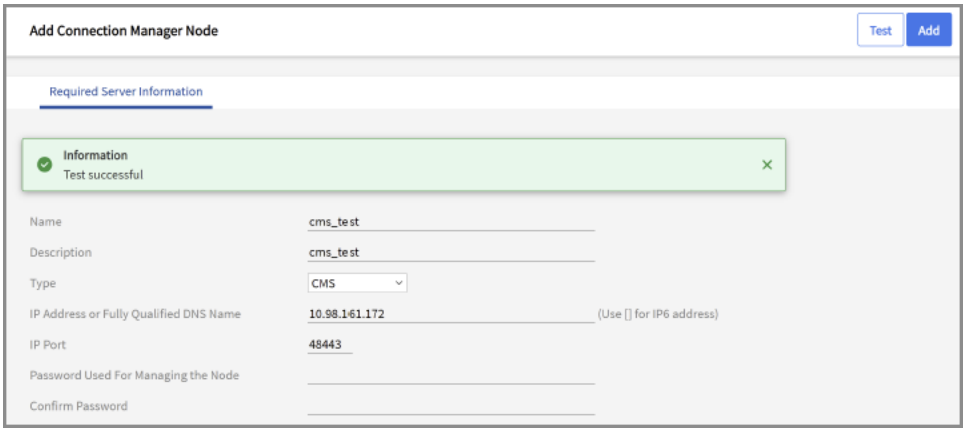
Click **Test** before adding the node to ensure that the type, IP address, IP port, and passwords are configured correctly.

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

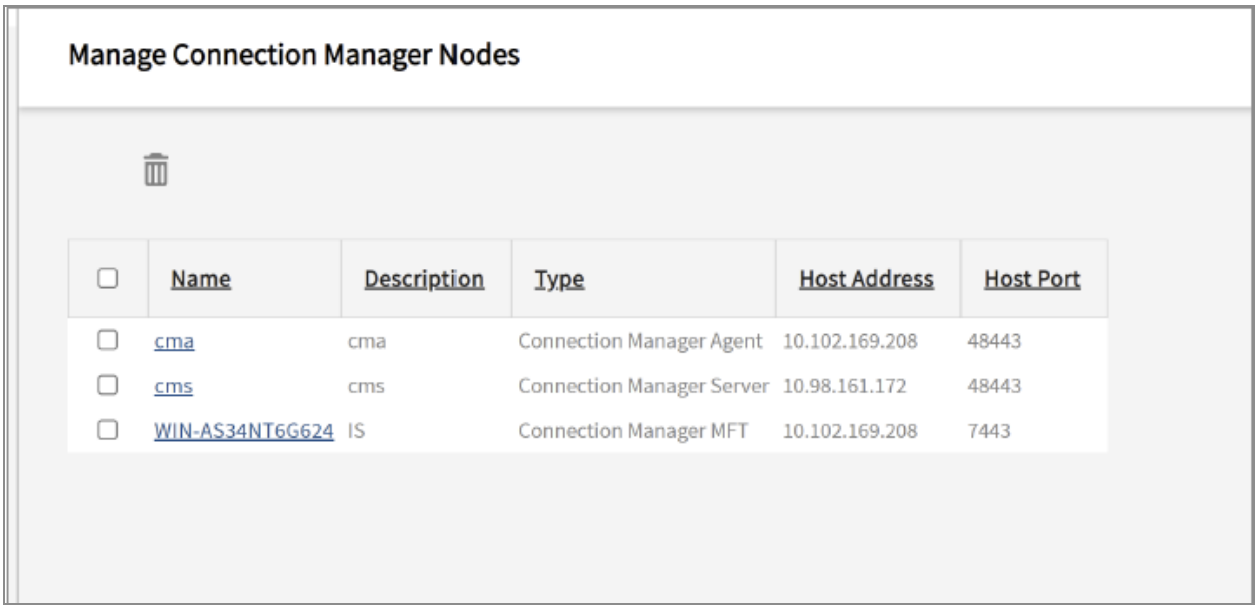


Click **Test** before adding the node to ensure that the type, IP address, IP port, and passwords are configured correctly.

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:

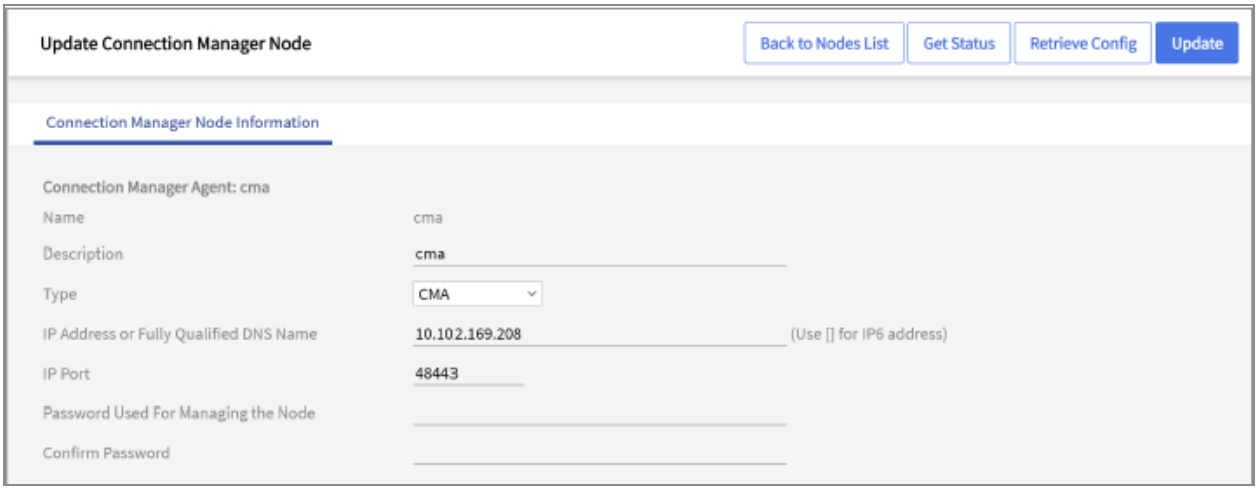


You can click an entry in the Name column in the **Results** table to get the detailed information for this node and update this node.

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

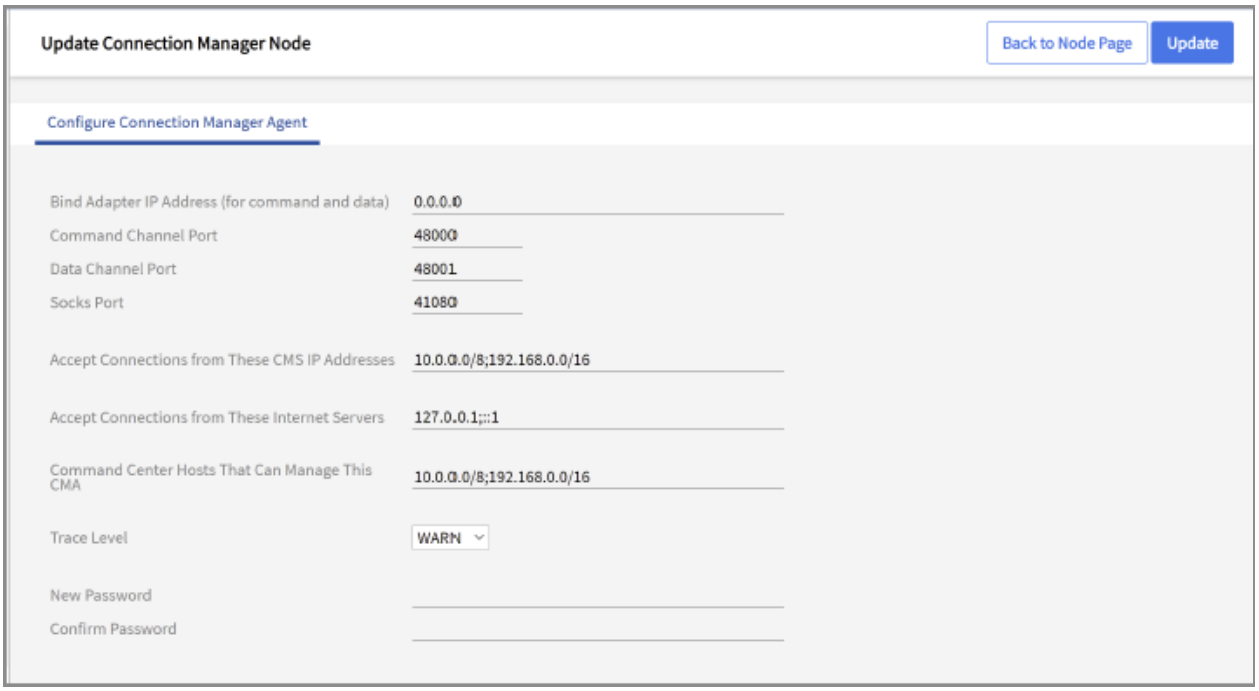
Updating CMA Configuration Information

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.



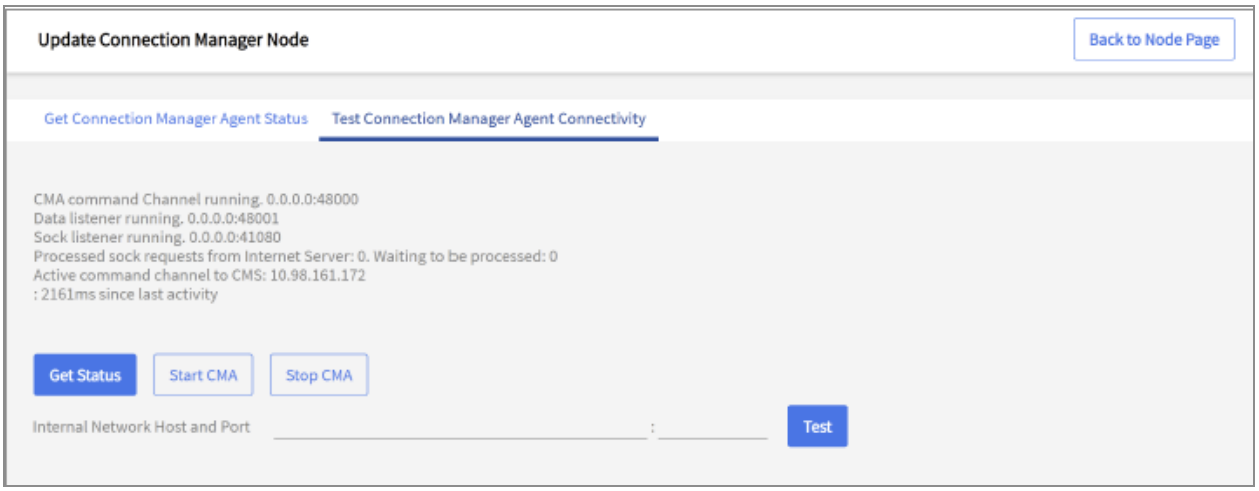
This page displays the configuration information for the Connection Manager node. You can update parameters and click **Update Config** to update the configuration.

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.



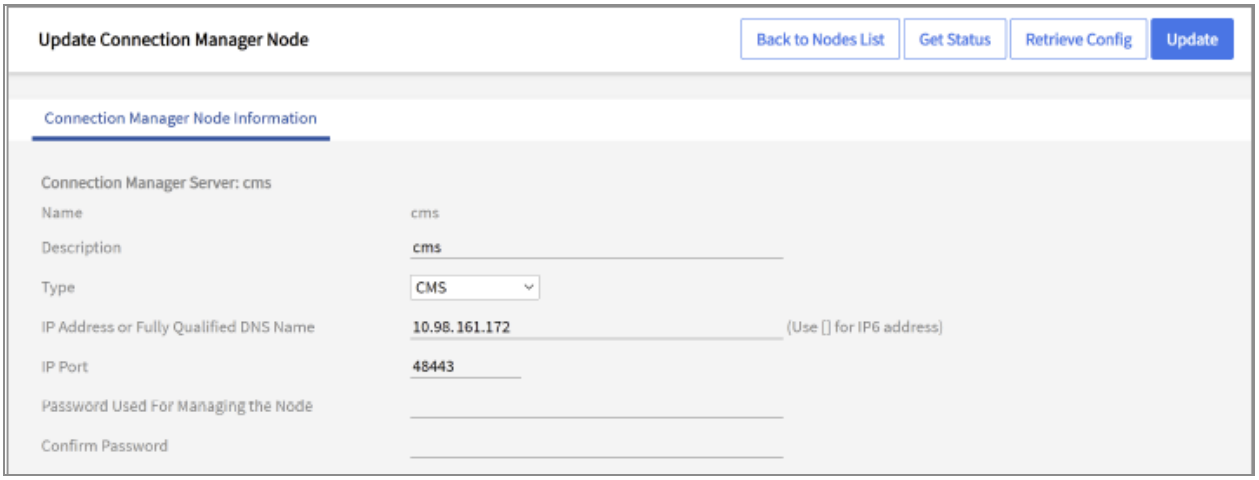
On this page, you can perform the following functions:

- **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.

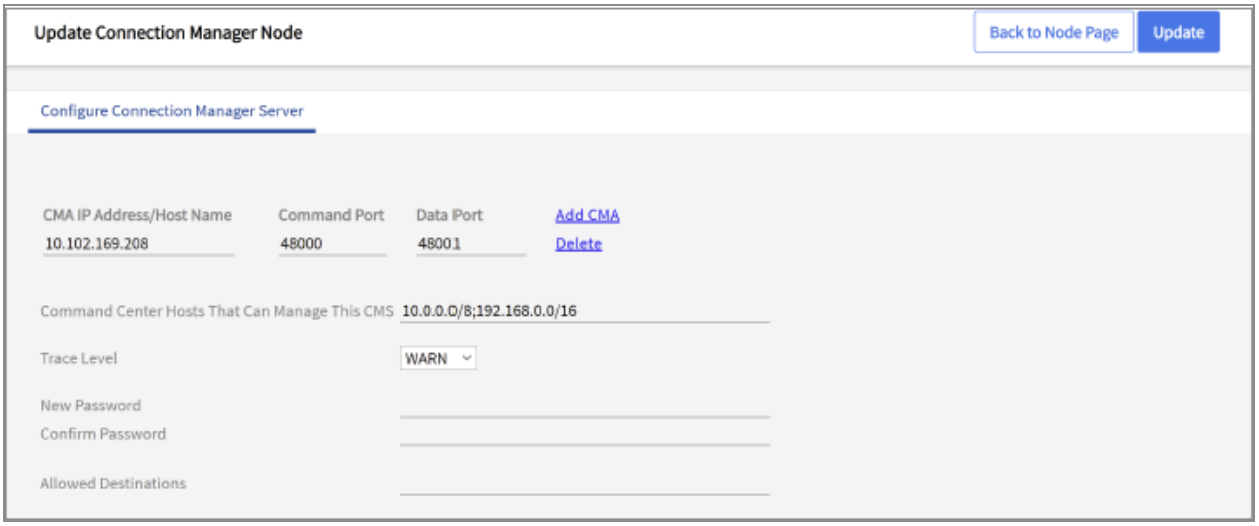
Updating CMS Configuration Information

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.

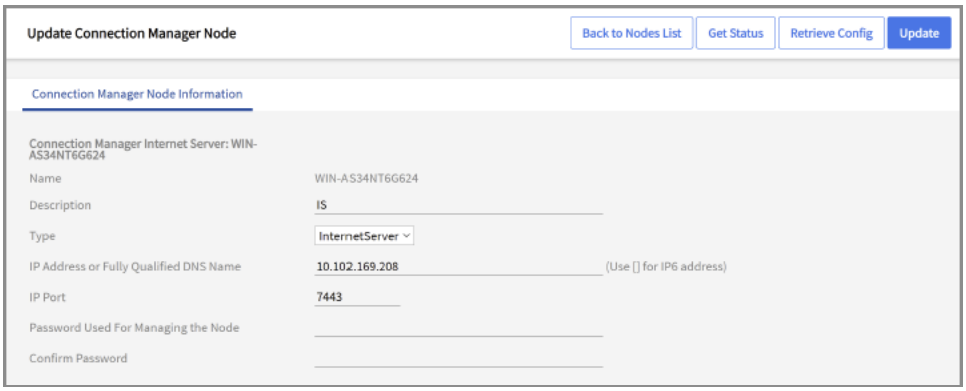
When you click **Get Status**, the following page is displayed showing the current status of the Connection Manager node.

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.

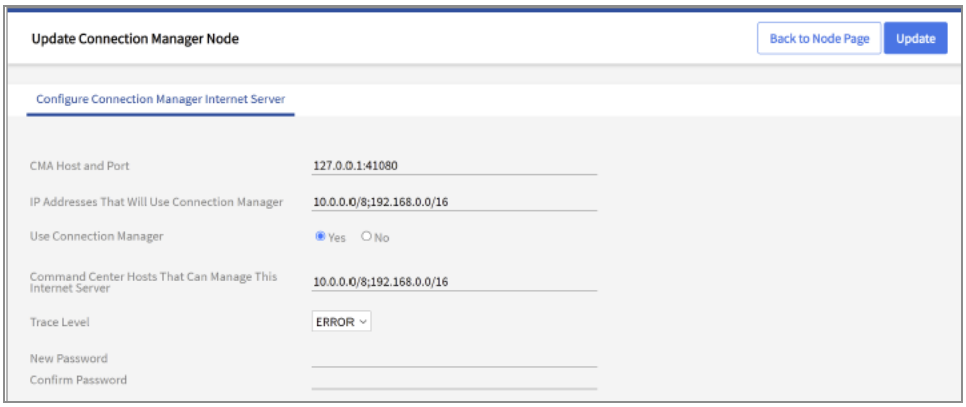
Updating Internet Server Configuration Information

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.

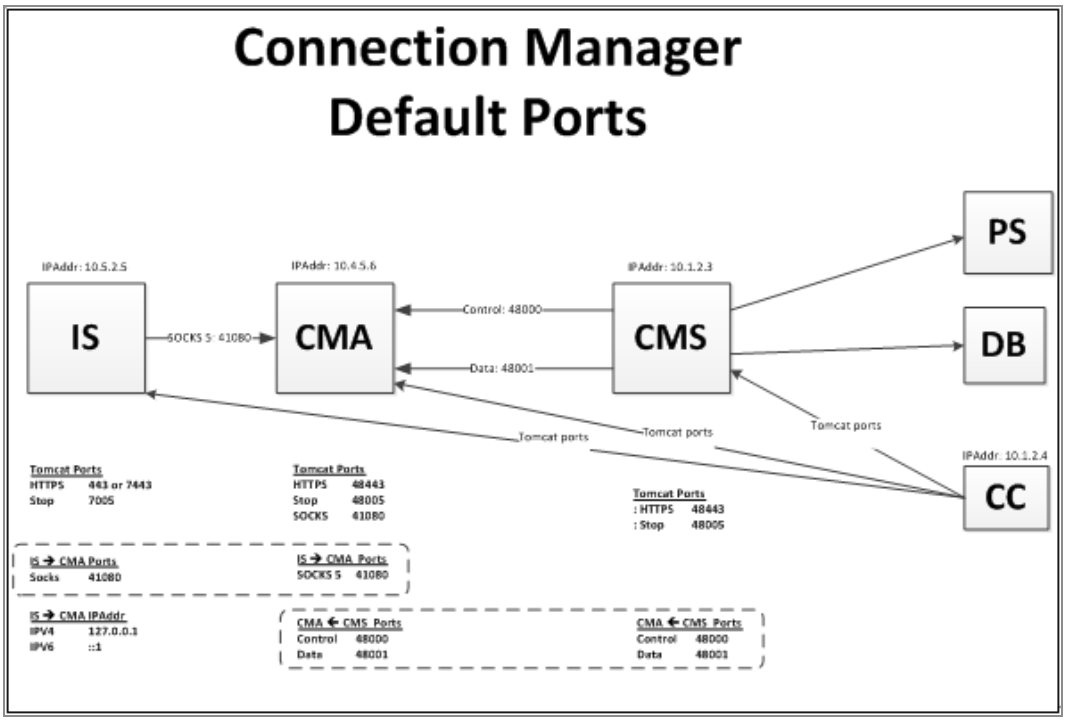
When you click **Get Status**, the following page is displayed showing the current status of the Connection Manager node.

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`: defines the load balance mode.
    - `aa` - active-active
    - `ap` - active-passive
    - `empty` - try other connections if the current connection is broken.

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/tempstore
```

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

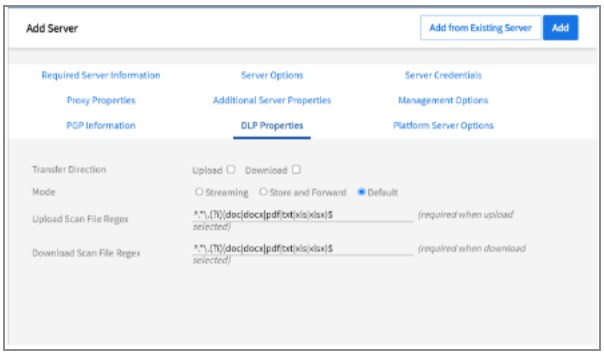
DLP settings on the **Transfer** definition override the DLP settings on the **Server** definition. By default, the **Transfer** definition uses the DLP settings from the **Server** definition.

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)$

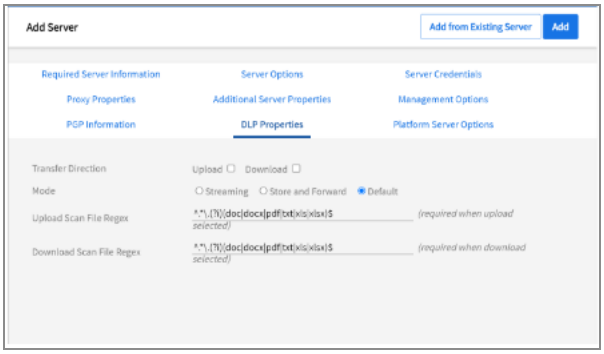
Note: The **Update Server** page has the same **DLP Properties** tab.

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.

Appendix E: Password Vault

To enhance the security of TIBCO® Managed File Transfer Command Center and TIBCO® Managed File Transfer Internet Server, instead of storing passwords and system keys in the MFT database, they can be stored in a Password Vault and retrieved when needed. MFT supports HashiCorp Password Vault and Azure Key Vault.

Password Vault Components

The following components can be stored in the Password Vault:

Servers

- Default Password
- Proxy Password
- DNI Password
- Google Cloud Auth File Content
- OFTP Local Password
- OFTP Partner Password

Server Credentials

- Remote Password

System Configuration

- Email Admin Password
- Cache Password
- ReCaptcha Secret Key

Platform Server Transfers

- Initiator Password
- Responder Password

Platform Server Profiles (User and Responder)

- Effective Password
- Responder/Incoming Password

Keys

- Private Key Password
- System Key (PGP, AS2, FTP, Platform Server, SSH, SAML, OFTP2, Kerberos Keystore)

LDAP Authenticators

- Bind Password

Configuring MFT Password Vault

To configure the Password Vault, on the System Configuration page, go to the **Password Vault Settings** tab.

The **Password Vault Settings** tab contains the following fields.

Field	Value
Enabled	Defines whether the Password Vault is enabled or not. When the Password Vault is disabled, MFT can still retrieve passwords located in the Password Vault server.
Vault Software	Selects the Password Vault server type. You can choose from the following two options:

Field	Value
	• Azure • HashiCorp
Server URL	Defines the IP Name or IP Address of the target Password Vault server. Sample URLs: • **Azure Key Vault:** `https://vaultname.vault.azure.net` • **HashiCorp Vault:** `https://hostname:port/v1/secret/data`
Azure Client Secret	Displayed only when using Azure Key Vault. Defines the client secret used to access the Password Vault. After you register your app with Azure, this field is available on the Azure portal.
Azure Client ID	Displayed only when using Azure Key Vault. Defines the Azure Client ID used to configure the Azure Key Vault. After you register your app with Azure, this field is available on the Azure portal.
Azure Tenant ID	Displayed only when using Azure Key Vault. Defines the Azure Tenant ID used to configure the Azure Key Vault. After you register your app with Azure, this field is available on the Azure portal.
Azure Object ID	Displayed only when using Azure Key Vault. Defines the Azure Object ID used to configure the Azure Key Vault. After you register your app with Azure, this field is available on the Azure portal.
Azure Secret ID	Displayed only when using Azure Key Vault. Defines the Azure Secret ID used to configure the Azure Key Vault. After you register your app with Azure, this field is available on the Azure portal.
Secret Expiration Email Recipient	Displayed only when using Azure Key Vault. Defines the email address where emails are sent before the Token or secret key expires. When the key is about to expire in 21 days or less, one email is sent everyday.

Field	Value
Trust All Certificates	Displayed only when using the HashiCorp Vault. Defines whether to allow all SSL and TLS certificates or only trusted certificates. You can select from the following two values: • **Yes:** All certificates, whether they use a trusted CA certificate or not, are trusted. Use this only for test environments. Ensure that only trusted CA certificates are used for the production environment. • **No:** Only trusted CA certificates are accepted. Use this as the default value for production environments.
Token	Displayed only when using the HashiCorp Vault. Defines the Token used to provide access to the Password Vault.
Token Expiration Email Recipient	Displayed only when using the HashiCorp Vault. Defines the email address where emails are sent before the Token or secret key expires. When the key is about to expire in 21 days or less, one email is sent everyday.
Default Name Prefix	Defines the prefix added to the name of the secret object. Ensure that this key is unique for each MFT cluster. **Important:** An MFT cluster includes all TIBCO MFT Command Center instances connecting to the same database. When connecting MFT Production, QA, and Development clusters to the same Vault server, define a different value for each MFT cluster.

Storage Location for Secrets

On the **System Configuration** page, you can set the storage location for MFT secrets, which include passwords and keys in the **Password Vault Settings** tab. You can choose to store secrets in either the vault or the database. It is a best practice to store all your secrets in the same location.

To choose the location, select either **Vault** or **Database** and click the Update button.

Once you have configured and enabled the Password Vault, MFT saves secrets in the specified location. Secrets are not moved in bulk. They are stored in the configured location only when added or updated.

To move all existing secrets between the database and the vault, click **Move to Database** or **Move to Vault**.

Use the **Status** button to see the number of secrets stored in the database. The Password Vault logs the results of the **move to the screen** to a log file located in the `<Installation Directory>/logs/message` directory, named `PasswordVault-YYYY-MM-DD.txt`.

> **Important:** Even after disabling the vault, MFT can still read secrets from it. You can also perform bulk movement of secrets after disabling the vault.

When the HashiCorp token or Azure secret token is about to expire in 21 days, one email is sent everyday to the configured recipient. The admin landing page also displays an informational message about the expiration.

Appendix F: Four Eyes

Four Eyes is an enhanced security model that ensures the confidentiality of highly sensitive data through a rigorous approval process. Every file transfer requires authorization before transmission to the recipient. The designated approver downloads, examines the file, and verifies the recipient. Once approved, the recipient is notified of the file's availability.

TIBCO MFT Internet Server and TIBCO MFT Command Center introduces **Four Eyes Policies** to implement this model. These policies designate user groups as approvers and recipients. The sender selects an approver and a recipient from these groups during transmission.

When the transfer definition is created, the sender can use the Four Eyes browser interface to select the file, designate an approver, and specify a recipient. The interface also allows the sender to include messages for both the approver and the recipient. After uploading the file, an email notification is sent to the approver. The approver then uses the same interface to download and examine the file. Once approved, an email is sent to the recipient to download the file. The recipient can use the Four Eyes browser interface to download the file.

To ensure privacy and security, MFT uses a separate repository for Four Eyes files, which should be located in a secure location.

Appendix G: Collection and Status Service - High Availability

The concepts defined in this appendix apply to both the Command Center Collection and Status Service features. This appendix describes the high availability concepts of the Collection Service. The same concepts can be applied to Status Service. Status Service is not discussed in this appendix. Use the Collection Service concepts as a guide to see how Status Service works.

The Collection Service is responsible for contacting platform servers to retrieve audit information on all completed transfers. The Collection Service collects audit records of file transfers from all platform servers when the Server definition **Manage Platform Server** checkbox is selected and the **Collect Platform Server History** parameter is set to `Initiator`, `Responder`, or `Both`.

The Collection Server can run in High Availability (HA) Active/Passive mode. Active/Passive HA means that the active server is collecting audit records from the platform servers and other TIBCO MFT Command Centers are in standby mode, waiting for the active server to stop. When the active Command Center Collection Service stops, one of the standby Command Center servers takes over and becomes the Active Collection server.

When running in HA mode, if the collection service stops running, the collection service automatically starts on a standby TIBCO MFT Command Center without user intervention.

For the Collector to run in HA mode, the following conditions must be met:

1. All TIBCO MFT Command Center servers selected to run the Collector must be at the version 8.5 level or above. If you select a TIBCO MFT Command Center server running versions 8.4 or earlier, the Collection Service runs in single server mode.
2. In the Configure Collection Service page, you must select more than one TIBCO MFT Command Center in the **Eligible Collector Server Hosts** parameter. The following ways are used to make multiple TIBCO MFT Command Center servers eligible to be the Collection server:
    - Select **All Command Centers** in the drop-down box. This option only exists when all TIBCO MFT Command Center servers are at the version 8.5 or higher

level.

- Select multiple TIBCO MFT Command Centers with versions 8.5 or higher servers in the drop-down box.

3. In the Configure Collection Server page, the service must be enabled.
4. The Service must be started through the Collection Server Status page.

Note: When running in HA mode, any of the servers eligible to be a collector can become the active collector.

Terms Used in This Appendix

Term	Description
HA	High Availability
Eligible Server	A server that is selected on the **Configure Collection Service > Eligible Collection Server Hosts** parameter.
8.4	This is any server running TIBCO MFT Command Center 8.4 0 or earlier version. This is important because the HA functionality was added to version 8.5 and is not available on version 8.4 or earlier versions.
8.5	This is any server running TIBCO MFT Command Center 8.5 0 or later. This is important because the HA functionality was added to version 8.5 and will be supported in future MFT versions.

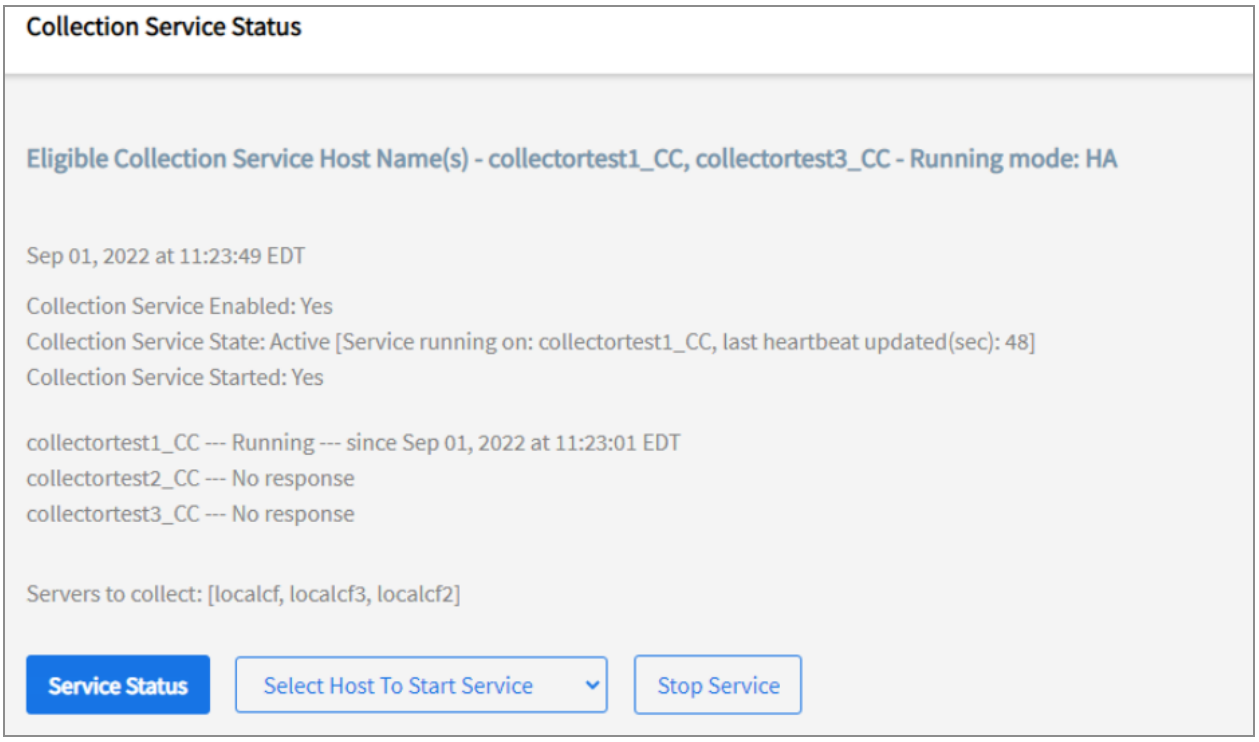
Collection Manager Web Pages

The following pages are used to configure and restart the Collection Service:

- Collection Service Status
- Configure Collection Service

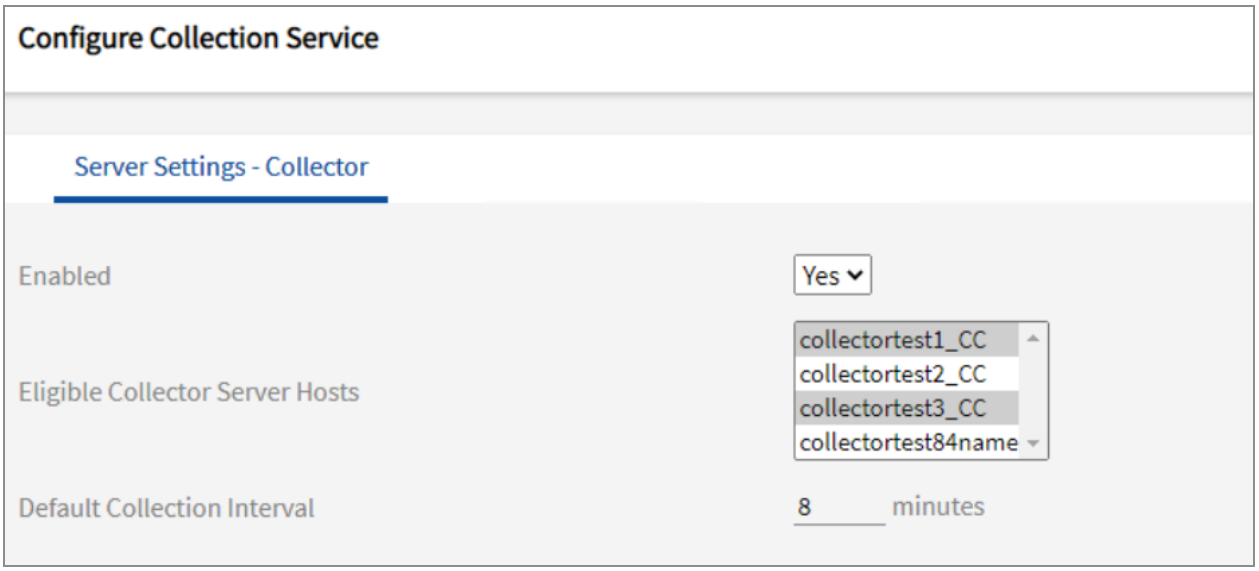
Collection Service Status

Go to **Management > Command Center Services > Collection Service > Collection Service Status**.



Configure Collection Service

Go to **Management > Command Center Services > Collection Service > Configure Collection Service**.



Differences between Collection in Versions 8.4 and Versions 8.5

These are the differences between Collection in versions 8.4 and versions 8.5.

Version 8.4

- When communicating to the Command Center versions 8.4, the Command Center admin issues servlet calls directly to the selected Command Center server and waits for a response.
- The Collection Service starts when the Collection Service is enabled and configured as the Collection server and when the MFT Command Center is started.
- The Collection Service (`Start`, `Stop`, and `Status`) are directed to the Server configured as the Collection Server.
- When a Start request is received, the Collection Service is started.
- When a Stop request is received, the Collection Service is stopped.
- When a Status request is received, Collection Service status is checked.
- Even when the Collector is started on version 8.4 or lower servers, the Command Center server issues asynchronous WebSocket calls to all Command Center version 8.5 servers and waits for a response when a status is requested.

Version 8.5

The Collection Service is started on all instances. The Collection Service continuously checks the following to determine when Collection should start on this server.

- When the **Configure Collection Service > Enable** parameter is set to `Enabled`.
- When this server is one of the servers selected in the **Configure Collection Service > Eligible Collector Server Hosts** parameter.
- When the Collection Service was started by the Admin clicking the **Collection Service Status > Start** button.
- The Collection Service (`Start`, `Stop`, and `Status`) are directed to all Command Center Servers, whether eligible or not eligible to be the collector.
- When a `Start` request is for a specific server, the Collection Service starts on that Command Center server.
- When a `Start` request is received for `Any Eligible Command Center`, the Command Center collector services compete to become the active Collector.
- When a `Stop` request is received, the Collection Service is stopped.
- When a `Status` request is received, Collection Service status is checked on all Command Center servers.
- When communicating to the Command Center version 8.5 servers, the Command Center admin issues WebSockets calls to all Command Center servers and waits for a response when the request is to retrieve status. The individual Command Center servers then use the database to determine if it should stop or start or Collector service.

This appendix discusses two different environments:

- Some Command Center servers are at version 8.4 or below
- All Command Center servers are running Version 8.5 or higher

Some Command Center Servers are at version 8.4

When some Command Center Servers are at version 8.5 and some are at version 8.4, High Availability depends on the servers selected to run the Command Center.

Collection does not run in High Availability mode when either of the following scenario occurs:

- When **Configure Collection Service > Eligible Collector Server Hosts** selects a version 8.4 server. When a version 8.4 server is selected, only one server starts the

Collection Service. Therefore, High Availability is disabled.

- When the Collection Service is running on a version 8.4 server, starting and stopping the Collection Service works the same as in version 8.4. Servlet calls are made directly to the selected server to start, stop, and get the status of the Collection Service.
- Asynchronous websocket calls are also made to the version 8.5 servers to update their status. The status for servers not eligible to run the Collector is typically `Not Eligible`.

Collection runs in High Availability mode when **Configure Collection Service > Eligible Collector Server Hosts** select multiple version 8.5 servers. Once the Collection Service is enabled and started, Collection HA is enabled. Command Center servers compete to become the active collector.

For more information on how multiple Command Center servers compete to become the active Collector, see Competing to become the Active Collector.

All Command Center Servers are at the 8.5 level

When all Command Center Servers are at version 8.5, High Availability depends on the Servers selected to run the Command Center.

Collection does not run in High Availability mode when **Configure Collection Service > Eligible Collector Server Hosts** selects only one Command Server. Since only one server is eligible to run the Collector, High Availability is not used. Even when only one server is eligible, the Collection thread is started on all Command Center instances. These instances monitor the database to determine if they have been made eligible to run the collector.

Collection runs in High Availability mode when either of the following scenarios occur:

- When **Configure Collection Service > Eligible Collector Server Hosts** select multiple version 8.5 servers. Once the Collection Service is enabled and started, Collection High Availability takes effect.
- Once Collection HA is enabled, Collection can be started on a specific server or on any eligible server.
- Starting Collection on a particular server. On the Collection Service Status, select a specific server from the **Start Service** drop-down menu.
- Starting Collection on any server. On the Collection Service Status, select `Any`

`Eligible Command Center` from the **Start Service** drop-down menu. Eligible Command Center servers compete to become the Active Collector.

For more information on how multiple Command Center servers compete to become the active Collector, see Competing to become the Active Collector.

Starting the Collection Server

You can start the Collection Service in any of the following ways:

1. Start the Collection Server on the Collection Service Status page. This starts the Collection Service on a particular server.
    a. Go to **Management > Command Center Services > Configure Collection Service**.
    b. Ensure that the **Configure Collection Service > Enabled** parameter is set to `Yes`.
    c. In the **Eligible Collector Server Hosts** parameter, select one or more Command Center servers.
    d. Command Center starts the Collection Server on the selected Command Center.
    e. When starting Collection on an MFT 8.4 Server, a servlet call is made to the target version 8.4 Command Center and an asynchronous WebSockets call is made to the version 8.5 servers.
    f. When starting Collection on an MFT 8.5 Server, an asynchronous WebSockets call is made to the version 8.5 servers.
2. Start the Collection Server using a REST call. When using the Start Service REST call, you cannot select an individual server where collection is started. It returns to the default value in `Any Eligible Command Center`.
3. Start the Collection Server on the **Collection Service Status** page. To start the Collection Server on a particular Command Center instance or on any eligible Command Center instance, click the **Start Service** button.

Note: When the Collection Service is started and you change the **Configure Collection Service > Eligible Collector Server Hosts**, the selected servers become the standby servers until the Active Collector server stops, and the eligible servers compete to become the Active Collection server.

If you remove the active Collection Server, the Collection stops on this server. If any other servers are selected, then they compete to become the active Collection Server.

If you selected additional Collection servers, the Collection Service could start on any of the selected servers.

Stopping the Collection Service

You can stop the Collection Service in any of the following ways:

1. Stop the Collection Server on the Collection Service Status page. This is how admins should stop the Collection service.

   Go to **Management > Command Center Services > Collection Service Status**.

   Click the **Stop Service** button.
   Command Center sends requests to all Command Center servers to stop the Collection Service. It could take up to 30 seconds for the Collection Service to stop.

2. Stop the Collection Server on the **Configure Collection Service** page. This method is less common. It is described so that admins understand the consequences of updating some of the fields in the **Configure Collection Service** page.

   Go to **Management > Command Center Services > Configure Collection Service.**

   There are two ways to stop the Collection from this page:

   a. Change the value of the **Enable** parameter from `Yes` to `No`. This prompts all of the eligible Command Center Collection servers that they should stop collection and stop competing to become the active Collection server. If the **Enable** value is changed back to `Yes`, the admin must start the Collection through the **Start** button on the **Collection Server Status** page.

   b. Clear the Current active Collection server from the list of "**Eligible Collector Server Hosts**.

      Note: If other hosts are defined in this parameter, another host competes to become the Collection Server.

Displaying the Collection Service Status

Go to **Management > Command Center Services > Collection Service Status**.

Click the **Service Status** button.

The Collection Server Status contacts all Command Center version 8.5 servers. It could take up to 10 seconds to get the collection status from all Command Center servers. Here are the possible Collection statuses for each Command Center:

- Initialization: The Collection Server is initializing
- Running: The Collection service is running
- Starting: The Collection Service is starting.
- Stopping: The Collection Service is stopping.
- Standby: The Collection Service is in standby mode, waiting for the Running Collection server to stop.
- Eligible: The Collection Service is eligible to run but the Collection Service has not started or is disabled.
- Not eligible: The Collection Service is not eligible to run.
- No response: No response was received from the Command Center server.

Competing to become the Active Collector

In order for Command Center to run the Collection Service in HA mode, you must select more than one Command Center server in the **Configure Collection Service > Eligible Collector Server Hosts** parameter. There are two times when eligible Command Center services compete to become the Active Collection service:

1. When the **Collection Service Status > Start Service** button is clicked and **Any Eligible Command Center** is selected. The Command Center servers detect that the collection service has started and since there is no active Collection server, the eligible Command Center servers compete to become the active collector.
2. When an active Collection Service is no longer responding and has exceeded the web.xml `ServiceInactivityThreshold` value, the eligible standby Command Center servers detect that the Active Collection server has exceeded the `ServiceInactivityThreshold` value and compete to become the active collector.

Logic to become the Active Collector Server

The Active Collection Server updates a heartbeat every minute. The Collection Server Status page shows the current heartbeat value. Each standby Command Center server checks the database every minute to detect if a Command Center is the active Collection Server. When the heartbeat has been inactive for the number of minutes defined in the

web.xml `ServiceInactivityThreshold` parameter (default is 5 minutes), this collector competes to become the active Collector.

Here is the logic that is executed:

- Attempt to create a lock on the **ServiceLock** database table.
- If another server has created this lock, then resume checking to detect when the Collector has become inactive.
- If the create lock was successful.
- Assume the role as the active Collector.
- Start the Collection thread to start collecting Platform Server Audit records.
- Release the lock on the **ServiceLock** database table.

Appendix H: License Key Validation

License Key Validation can be performed with the environment variables:

```
TIB_ACTIVATION
```

If the environment variables are not defined, it checks the `mft-license.properties` file. `mft-license.properties` file is created during installation and is placed in `{IS_OR_CC}/server/webapps/cfcc/WEB-INF` folder. `mft-license.properties` contains below data:

```
TIB_ACTIVATION
```

This field is required to validate the license in two different ways:

1. **Server validation**:

   The Activation Server should be installed on the client machine, and the license file should be uploaded to the server. To test server validation, we have to specify the license server url in `TIB_ACTIVATION` property in `mft-license.properties` or `TIB_ACTIVATION` environment variable.

2. **License File Validation**:

   Generate a license file and ensure that it is the only file in the specified directory. To validate the file, add the directory path of the license file in the `TIB_ACTIVATION` property in the `mft-license.properties` file or set the path in the `TIB_ACTIVATION` environment variable.

License Validation is performed at server startup. If the license is valid for more than 7 days, the validation runs every 24 hours. If the license validity is 7 days or less, the validation occurs every hour.

Check the below log files for all the logs related to MFT license:

- license-message-yyyy-mm-dd.txt in logs/messages folder
- license-trace-YYYY-MM-DD.txt in server/logs folder

The user can change the values of mft-license.properties placed in {IS_OR_CC}/server/webapps/cfcc/WEB-INF folder. To access the updated license information, the Tomcat server should be restarted. Applying a new license on the activation server or

adding a new license file in the local license directory does not require a restart of MFT. These changes will be reflected in the next validation cycle.

License information can be accessed in the following pages after the user logs into the Command Center and Internet Server Admin:

- **License** tab on the header of the page.
- **License Information** in the Diagnostics page.

Note: License Expiration Date and **Last Connection Date** information can be found in these pages.

License Email Notification Address and **License Email Template** can be configured in the **System Configuration** page. If the **Email Notification** is configured, an email notification is sent when the **License Expiration Date** is less than or equal to 90 days or when the license is invalid.

License Expiration Warnings

TIBCO Managed File Transfer Command Center validates the license at startup and once per day. Validation uses either the activation service URL or the local license file based on the activation type used to activate your product.

Duration from expiration	Notification/Alert frequency	Message
90 days or less	One notice notification is pushed once per day.	`NOTICE: Entitlement to {product-name} for {customer-name} ends on {expiration-date}, at which time product shutdown will occur. Renew your entitlement as soon as possible.`
7 days or less	One alert notification is pushed once per hour.	`ALERT: {product-name} will shutdown on {expiration-date} when entitlement ends for {customer-name}. Renew your entitlement immediately to avoid product shutdown.`
0 days (on expiration)	An error notification is pushed and the Platform Server for	`ERROR: Entitlement to {product-name} for {customer-name} has ended. Renew your entitlement immediately to resume product usage.`

	Windows service shuts down.

Note: Your license includes a grace period, allowing MFT Command Center to run for a limited time even when it cannot reach the activation server. Once this grace period expires, an error notification is sent and the server automatically shuts down.

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 Product Documentation website, mainly in HTML and PDF formats.

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

Product-Specific Documentation

The documentation for this product is available on the TIBCO® Managed File Transfer Command Center Documentation page.

How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our product Support website.
- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the product Support website. If you do not have a username, 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

SOME CLOUD SOFTWARE GROUP, INC. (“CLOUD SG”) SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, “INCLUDED SOFTWARE”). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

TIBCO, the TIBCO logo, the TIBCO O logo, and Slingshot are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG’s Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: https://scripts.sil.org/OFL

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the “readme” file for the availability of a specific version of Cloud SG software on a specific operating system platform.