Informatica® Managed File Transfer
10.4.0

Informatica Managed File Transfer Installation Guide

Informatica Managed File Transfer Informatica Managed File Transfer Installation Guide
10.4.0
December 2020

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2020-12-21

Table of Contents

Preface

Follow the instructions in the *Managed File Transfer Installation and Configuration Guide* to install, configure, upgrade, and back up Managed File Transfer. The guide also includes pre-installation notes about database requirements, user accounts, the usage of port numbers, and browser compatibility, and provides instructions for customizing the installation settings and for starting and stopping Managed File Transfer.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

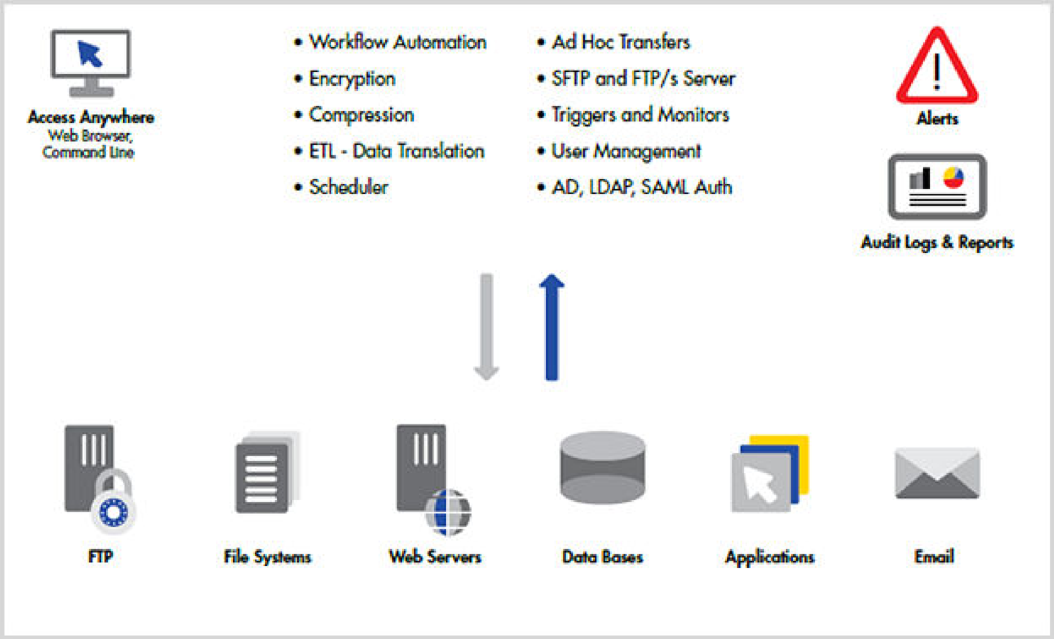
To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Introduction

Informatica Managed File Transfer provides centralized control and auditing of file transfers and workflows for the enterprise. With its comprehensive features and intuitive interface, Managed File Transfer can reduce operational costs, improve the quality of data transmissions and meet stringent compliance requirements.

The following figure shows the Managed File Transfer capabilities:



Note: You must use Managed File Transfer with Informatica B2B Data Exchange or Informatica Cloud B2B Gateway. You cannot use Managed File Transfer features independently of B2B Data Exchange or Cloud B2B Gateway. Also, you cannot use Managed File Transfer for any operations other than file transfer operations.

For more information, see the Statement of Support.

Managed File Transfer General Features

- Includes a browser-based administrator interface with a customizable dashboard, advanced graphical components and drag-n-drop support.
- Supports popular file transfer protocols including SFTP, SCP, FTP/s, HTTP/s, AS2, Web Services, SMTP, POP3 and IMAP.

- Provides client components for connecting to internal and external systems for sending and retrieving files.
- Provides server components to allow systems and users to connect to Managed File Transfer for uploading and downloading files.
- Logs all file transfer activity in a central database with an optional SYSLOG feed.
- Produces a wide variety of management and analytical reports.
- Allows clustering for high availability (active-active) and load balancing.
- Controls user access with role-based permissions and extensive security controls.
- Includes key management tools for Open PGP Keys, SSH Keys and SSL Certificates.
- Works with the optional Managed File Transfer Gateway to keep files out of the DMZ and close inbound ports into the internal (private) network.

Managed File Transfer can be used for a variety of file transfer needs including workflow automation, ad-hoc file transfers and document collaboration. It can simplify system-to-system, user-to-system and user-to-user file transfers.

Workflow Automation

- Provides a graphical interface for creating multi-step workflows; no scripting or programming required.
- Includes an integrated scheduler for running workflows and file transfers at future dates/times.
- Triggers workflows based on events, such as an upload/download event or the presence of a new file in a folder.
- Provides APIs and commands for running workflows from customer applications and 3rd party schedulers.
- Encrypts, signs, verifies and decrypts files using the Open PGP encryption standard.
- Accesses files and directories on network shares with support for UNC, NFS, SMB and CIFS.
- Connects to popular database servers SQL Server and Oracle.
- Translates data to/from Excel, XML, Delimited text and Fixed Width file formats.
- Calls customer programs and scripts as part of an overall workflow.
- Connects to enterprise messaging systems including Websphere MQ, SonicMQ, ActiveMQ and SwiftMQ
- Compresses and extracts files using ZIP, GZIP and TAR standards.
- Supports large files with auto-resume and integrity checks to help guarantee delivery.
- Allows workflow jobs to be prioritized and segmented with job queues and run priorities.
- Sends email alerts and text messages for failed and completed transfers.

Ad-Hoc File Transfers and Collaboration

- Provides an HTTPS web-client for browser-based file transfers.
- Allows access to authorized network folders through the browser.
- Includes the Shared Drive file system for collaboration, sharing and synchronizing documents across devices.
- Provides delivery of sensitive messages and documents through email notifications with secure HTTPS links.

- Integrates with Active Directory (AD), LDAP and SAML for user authentication
- Allows self-registration of users with administrator approval.

Administration

Authorized users can utilize the Managed File Transfer browser-based Administrator to perform configuration and monitoring within the product.

CHAPTER 2

Pre-Installation Notes

This chapter includes the following topics:

Verify the Database Requirements

Verify that your database meets the requirements for running Informatica Managed File Transfer .

The following table describes the database requirements for Managed File Transfer:

Database Component	Description
Database System	Type of database on which to install the repositories. You can use one of the following database systems: - Oracle - Microsoft SQL Server
Disk space	The database requires at least 512 MB of disk space for the core application. You also need additional space based on the number of messages that you need to process and the type of processing required. The frequency of message archiving also affects the disk space requirement.
Database connections	One or more database connections must always be available. The number of required connections depends on the number of endpoints and the number of documents processed concurrently. Use the following formula to calculate the number of required database connections : (NumberOfEndpoints + Maximum number of concurrent processes + 3) X 3 + 2 If you do not have enough database connections available, processing might fail or you might encounter database deadlocks. The default number of database connections is 2.

Database Unicode Support

If you require Unicode support, create the repository database with the following settings:

- Oracle databases: use the AL32UTF8 Unicode character set.
- Microsoft SQL Server: it is recommended that you use data types that support Unicode data: nchar, nvarachar, and ntext.

Microsoft SQL Server Collation

If you use Microsoft SQL Server, the collation for the repository must not be case sensitive.

Database User Accounts

Before you install, verify that you have the user names and passwords for the required database and domain accounts.

The following table describes the required user accounts:

User Account	Description
Database	Database user account that you use to log in to the database server and create tables and views for the repository. You must install all the repositories on the same type of database server. You must create a separate user account for each repository. The user accounts must have privileges to perform the following actions: - Select data from tables and views. - Insert data into tables, delete data from tables, and update data in tables. - Create, change, and delete the following elements: - Tables - Views - Synonyms - Indexes - Custom data types - Triggers - Create, change, delete, and run stored procedures and functions. If you use a Microsoft SQL Server database, you must set up separate databases for each repository. It is recommended that you grant database owner privileges to the user accounts.
If you use Managed File Transferwith Informatica domain authentication: Informatica domain administrator	Administrator account for the Informatica domain.
If you use Managed File Transfer with Informatica domain authentication: Informatica security domain	User account for Informatica domain authentication. The user account must be created in the Informatica Administrator tool with the **manage roles/groups/users** privileges. The Managed File Transfer administrator synchronizes the user account after the installation.

Port Number Usage

Managed File Transfer will utilize port numbers on the server for its various modules. Listed below are the default port numbers that will be used.

Port Number	Description
8000	Administrator functions over HTTP
8002	Administrator functions over HTTPS
8005	Shutdown port for Managed File Transfer
8006	Clustering communications channel (if enabled)
443	HTTPS/AS2 service for trading partners
21	FTP service for trading partners
990	FTPS service for trading partners
22	SFTP service for trading partners

These port numbers can be overridden either during the installation or at any time after the installation.

Browser Compatibility

The Managed File Transfer Administrator and File Transfer Portal interface's require modern internet browsers that support HTML 5. Internet Explorer and Chrome are supported. Some HTML 5 advanced features, such as drag and drop, will not work in older versions of browsers.

CHAPTER 3

Installation and Configuration

This chapter includes the following topics:

Windows Installation

Managed File Transfer can be installed onto a Windows server for enterprise usage. Managed File Transfer can also be installed onto Windows desktops or laptops, which is useful for individual development and testing purposes. 64-bit versions of Windows are supported.

A Windows installation wizard is provided for Managed File Transfer which installs the product files into the directory of your choice. Managed File Transfer will be implemented as a Windows Service which will automatically start (by default) when Windows starts.

Requirements

The following requirements apply to a Windows installation.

Item	Requirement
Disk space	600 MB (does not include user data)
Memory	512 MB minimum

Installing Managed File Transfer on Windows

Perform the following steps to install the Managed File Transfer product on a Windows machine.

1. Login to the target Windows system as an administrator.
2. Download the Managed File Transfer installer `Install.exe` file.
3. Execute the downloaded `Install.exe` file and follow the prompts on the screens.

4. To start the Managed File Transfer application server perform the following instructions:
    a. Go to **Control Panel** > **Administrative tools** > **Services**.
    b. In the Services window, right-click on **Informatica MFT 10.2.3** and select **Start**.
    c. Within seconds after starting Managed File Transfer, its status should be updated to "Started". If not, contact Informatica Support.
5. The installation and startup of Managed File Transfer is complete. For configuration instructions, see "Initial Configuration " on page 20.

Note: Managed File Transfer is configured in Windows as an automatic startup Service. This means that the Managed File Transfer will automatically start whenever Windows starts.

UNIX Installation

Managed File Transfer can be installed onto a server for enterprise usage.

An installation wizard is provided for Managed File Transfer which installs the product files into the directory of your choice.

Requirements

The following requirements apply to a UNIX installation.

Item	Requirement
Disk space	600 MB (does not include user data)
Memory	512 MB minimum
JRE (Java Runtime Environment)	1.8 or higher

Note: For an AIX installation, you need to have JRE 1.8 SR2 FP10 installed.

Installing Managed File Transfer

Perform the following steps to install Managed File Transfer onto a UNIX server.

1. Create or designate a non-root user on the system that will be used to install and run the Managed File Transfer application. This user will be the owner of all files created during installation as well as files written to the file system during use.
2. Login to the server.
3. Download the Managed File Transfer UNIX installer `Install.bin` file.
4. Open a Terminal window.
5. Change the directory to where the installer file was downloaded.
6. Run the installer.
7. Follow the on-screen instructions to complete the installation.

8. Start the Managed File Transfer by following these instructions:
    a. Open a Terminal window.
    b. Change the working directory to the tomcat directory where Managed File Transfer is installed, for example `Opt/Informatica/B2B/MFT/server/tomcat/bin`.
    c. Start the Managed File Transfer by executing the following command: `mft-server.sh` start.
9. The installation and startup of Managed File Transfer is complete. For configuration instructions, see "Initial Configuration " on page 20.

    You can setup Managed File Transfer so it starts automatically when the system is booted. Refer to your operating system manual for more details on setting up auto-start services.

Installing Managed File Transfer on a Silent Mode

To install Managed File Transfer without user interaction, install in a silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install Managed File Transfer on multiple machines on the network or to standardize the installation across machines.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

To install in silent mode, complete the following tasks

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.
3. Secure the passwords in the installation properties file.

Configuring the Installer Properties for Managed File Transfer

The installation properties file includes the parameters that are required by the installer.

The following table describes parameters that you add in the installation properties file:

Parameter	Description
Specify whether to install or upgrade Managed File Transfer.	
IS_INSTALL	To install Managed File Transfer, set the parameter to 1.
IS_UPGRADE	To upgrade Managed File Transfer, set the parameter to 1.
Configure the components to install using the following parameters	
ADD_COMPONENTS=0	To add all Managed File Transfer components, set the parameter to 1.
MFT_SERVER=1	To add Managed File Transfer server component, set the parameter to 1.

Parameter	Description
MFT_GATEWAY=1	To add Managed File Transfer Gateway component, set the parameter to 1.
MFT_CMD_TOOL=1	To add Managed File Transfer command line utility component, set the parameter to 1.
Configure PowerCenter version using the following parameters:	
PWC_VERSION_1020_OR_ABOVE	To use the PowerCenter version later to 10.2.0 or above, set the parameter to 1.
PWC_VERSION_EARLIER_THAN_1020	To use the PowerCenter version earlier to 10.2.0, set the parameter to 1.
Configure the installation directory using the following parameter:	
USER_INSTALL_DIR	Absolute path to the installation directory
Configure the Managed File Transfer repository using the following parameters:	
BLANK_USER	To create a new Managed File Transfer repository, set the parameter to 1.
CONFIGURED_USER	To use an existing Managed File Transfer repository, set the parameter to 1.
DB_TYPE_1	Type of database to use for the Managed File Transfer metadata repository. Enter either of the following options: - Oracle - Microsoft SQL Server
DB_CONNECTION_STRING_1	To use a custom connection string, set the parameter to 1.
DB_HOST_1	Host name of the machine where the database server is installed.
DB_PORT_1	Port number for the database. The default port number for Oracle is 1521. The default port number for Microsoft SQL Server is 1433.
DB_SID_1	System identifier for the database if the database is Oracle. Enter a fully qualified Service Name or a fully qualified SID.
DB_CONNECTION_STRING_VALUE_1	The value of the connection string. Configure one of the following connection strings: - JDBC connection string - ODBC connection string
DB_WINDOWS_AUTHENTICATION_1	To authenticate user names against the Microsoft Windows authentication mechanism, set the parameter to 1.
DB_USER_1	Name of the database user account for the database where you do not use Windows authentication.

Parameter	Description
DB_PASSWORD_1	Password for the database account for the database where you do not use Windows authentication. Managed File Transfer stores the password as an encrypted string.
DB_ODBC_STRING_VALUE_1	Value of the ODBC connection string.
Configure the Managed File Transfer port numbers using the following parameters:	
MFT_PORT_VARIABLE_ADMIN	Port to use for the admin user. Set the parameter to 8000.
MFT_PORT_VARIABLE_SECURE_ADMIN	Port number to use for the secure admin user.
MFT_PORT_VARIABLE_HTTPS	Port number for the HTTPS hosted service.
MFT_PORT_VARIABLE_FTP	Port number for the FTP hosted service.
MFT_PORT_VARIABLE_FTPS	Port number for the FTPS hosted service.
MFT_PORT_VARIABLE_SFTP	Port number for the SFTP hosted service.
MFT_PORT_VARIABLE_MLLP	Port number for the MLLP hosted service.
MFT_PORT_VARIABLE_SHUTDOWN	Port number for the Managed File Transfer server shutdown listener.
Configure the Managed File Transfer Gateway ports using the following parameters:	
GATEWAY_CONTROLLER_ADDRESS	IP address for the Managed File Transfer Gateway controller address.
GATEWAY_CONTROLLER_PORT	Port number for the Managed File Transfer Gateway port.
GATEWAY_DATA_ADDRESS	IP address for the Managed File Transfer Gateway data address.
GATEWAY_DATA_PORT	Port number for the Managed File Transfer Gateway data port.
GATEWAY_SHUTDOWN_PORT	Port number for the Managed File Transfer Gateway shutdown port.
Configure the Managed File Transfer Gateway proxy using the following parameters:	
GATEWAY_PROXY_ENABLED	To enable theManaged File Transfer Gateway proxy set the parameter to 1.
GATEWAY_PROXY_ADDRESS	IP Address for the Managed File Transfer Gateway proxy.
GATEWAY_PROXY_PORT	Port number for the Managed File Transfer Gateway proxy.
GATEWAY_FORWARD_PROXY_ADDRESS	IP address of the Managed File Transfer Gateway forward proxy.
GATEWAY_PASSIVE_PROXY_ADDRESS	IP address of the Managed File Transfer Gateway passive proxy.

Parameter	Description
GATEWAY_PASSIVE_PROXY_FROM_PORT	Starting port number of the Managed File Transfer Gateway proxy.
GATEWAY_PASSIVE_PROXY_TO_PORT	End port number of the Managed File Transfer Gateway proxy.

Sample of the Installer Properties Configuration for MFT

Use the following sample to configure the installation properties file to install Managed File Transfer in a silent mode:

```
#Install or Upgrade
#-------------------
IS_INSTALL=1
IS_UPGRADE=0

#Installation Directory
#-----------------------
USER_INSTALL_DIR=/data/Informatica/B2B

#Installation Components
#------------------------
ADD_COMPONENTS=0
MFT_SERVER=1
MFT_GATEWAY=1
MFT_CMD_TOOL=1

#Power Center Version selection
#-------------------------------
PWC_VERSION_1020_OR_ABOVE=1
PWC_VERSION_EARLIER_THAN_1020=0

#Informatica Managed File Transfer Repository
#--------------------------------------------
BLANK_USER=1
CONFIGURED_USER=0
DB_TYPE_1=Oracle
DB_CONNECTION_STRING_1=0
DB_USER_1=MFT_Repo_User
DB_PASSWORD_1=MFT_Repo_User
DB_HOST_1=localhost
DB_PORT_1=1521
DB_SID_1=orcl
DB_CONNECTION_STRING_VALUE_1=jdbc:informatica:oracle://localhost:1521;SID=orcl;
DB_WINDOWS_AUTHENTICATION_1=0
DB_ODBC_STRING_VALUE_1=jdbc:informatica:oracle://localhost:1521;SID=orcl;

#Informatica Managed File Transfer Port Numbers
#----------------------------------------------
MFT_PORT_VARIABLE_ADMIN=8000
MFT_PORT_VARIABLE_SECURE_ADMIN=8002
MFT_PORT_VARIABLE_HTTPS=443
MFT_PORT_VARIABLE_FTP=21
MFT_PORT_VARIABLE_FTPS=990
MFT_PORT_VARIABLE_SFTP=22
MFT_PORT_VARIABLE_MLLP=2575
MFT_PORT_VARIABLE_SHUTDOWN=8005

#Informatica Managed File Transfer Gateway Ports
#-----------------------------------------------
GATEWAY_CONTROLLER_ADDRESS=127.0.0.1
GATEWAY_CONTROLLER_PORT=9100
GATEWAY_DATA_ADDRESS=127.0.0.1
```

```
GATEWAY_DATA_PORT=9101
GATEWAY_SHUTDOWN_PORT=9105

#Informatica Managed File Transfer Gateway Proxy Ports
#------------------------------------------------------
GATEWAY_PROXY_ENABLED=1
GATEWAY_PROXY_ADDRESS=127.0.0.1
GATEWAY_PROXY_PORT=9102
GATEWAY_FORWARD_PROXY_ADDRESS=127.0.0.1
GATEWAY_PASSIVE_PROXY_ADDRESS=127.0.0.1
GATEWAY_PASSIVE_PROXY_FROM_PORT=30000
GATEWAY_PASSIVE_PROXY_TO_PORT=32000
```

Running the Managed File Transfer Silent Installation

Before you run the installer in the silent mode, ensure that you configure the installer configuration file:

1. Configure the installation properties in a text file.

   Note:

   - For more information about parameters to configure in the installer properties file, refer to GUID-A807977B-0FCF-42A0-83E8-2195D05F5A34.
   - For using a sample of the installer properties file, refer to GUID-997BBC8D-337A-4889-AB41-06406E0A5909.

2. Run the following command in the command prompt to silent install B2B Data Exchange using the installer properties file:

   - If you use the Windows operating system, run the following command:
     `Install.exe -f <location>/installer.properties -i silent`
   - If you are using the UNIX operating system, run the following command:
     `./Install.bin -f <location>/installer.properties -i silent`

   Where `<location>` is the location of the file that contains the installer properties.

   For example, the location of the file that contains the installer properties might be:

   ```
   /data/username/installers/1023/MFT
   ```

The silent installer runs in the background.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

Initial Configuration

Follow the instructions below to test the installation and perform initial configuration of Managed File Transfer.

1. To access the Managed File Transfer Administrator using a standard HTTP connection, open your browser and type the URL of `http://[hostname]:[portnumber]` where `[hostname]` is the host name or IP address of the Managed File Transfer and `[portnumber]` is the port number of the Managed File Transfer Administrator. The default HTTP port for the Administrator is 8000, for example: `http://myserver:8000`

   Otherwise, to access the Managed File Transfer Administrator over a secure HTTPS connection, open your browser and type the URL of `https://[hostname]:[portnumber]`. The default HTTPS port for the Administrator is 8002, for example: `https://myserver:8002`.

2. Login with your user name and password. The default user name and password is `Administrator`.
3. The Managed File Transfer Administrator dashboard is displayed.
4. Review and adjust the global settings in Managed File Transfer by following the instructions below:

    a. From the main menu bar, select the **System** option.

    b. Choose the **Global Settings** option.

    c. Review the settings on the tabs and make any changes as needed. Read the on-line help text ? for each setting to understand its purpose.

    d. Be sure to specify the settings for your SMTP server on the **SMTP Settings** tab. This will allow Managed File Transfer to send email alerts when certain events occur.

    e. Note that some changes to the Global Settings will take effect only when Managed File Transfer is restarted.

5. By default, Admin User and Web User passwords are authenticated against the passwords stored in the Managed File Transfer database. Optionally, you can configure Managed File Transfer Login Methods for basic authentication of Admin User and Web User passwords against a Windows Active Directory or Generic LDAP located within your organization. Web User accounts can also be synchronized with users stored in an LDAP server.

    a. From the main menu bar, select the **Users** option.

    b. Choose the **Login Methods** option.

    c. Click the **Add Login Method** button.

    d. Read the on-line help text ? for specific instructions to configure user authentication for your system.

6. The passwords for the included administrator and root user ids will always be authenticated against Managed File Transfer internal database. For security purposes, you should change the passwords for these users by following the instructions below.

    a. From the main menu bar, select the **Users** option.

    b. Choose the **Admin Users** option.

    c. Next to the administrator user name, click on the ⚙button and choose 🔒 Reset password.

    d. Key in the new password on the screen and click on the **Reset** button.

    e. Next to the root user name , click on the ⚙button and choose 🔒 Reset password.

    f. Specify the new password on the screen and click on the **Reset** button.

    g. Record the new passwords in a safe place.

7. Manage the settings for the services, such as FTP, FTPS, SFTP, HTTPS, AS2, which you want to make available to your trading partners by following the instructions below:

    a. From the main menu bar, select the **Services** > **Service Manager**.

    b. Follow the instructions in the on-line help ? to learn how to adjust settings for the various services.

    c. After adjusting any settings, you can click on the ▶ icon to start (or restart) the service.

To backup configurations and settings, which should be performed on a regular basis, see “Backups” on page 44. To set firewall settings, see “Firewall Recommendations ” on page 31.

CHAPTER 4

Customizing Installation Settings

This chapter includes the following topics:

Changing Managed File Transfer Port Numbers

By default, Managed File Transfer administrator will utilize port numbers 8000, 8002 and 8005 on your system for the following functions:

- 8000 is the default HTTP port which users can connect (from their browsers) for performing administration in Managed File Transfer.
- 8002 serves the same function as port 8000, but uses a HTTPS (SSL-protected) connection.
- 8005 is the default port for requesting a shutdown of Managed File Transfer from a remote system.

You can change these port numbers within the Managed File Transfer browser-based administrator interface.

Changing Ports with the Browser

1. Open a browser window and log into the Managed File Transfer Administrator.
2. From the main menu bar, select **System** > **Admin Server Configuration**.
3. Select the **Listener** node in the tree.
4. Specify the new port number and click on the **Save** button.
5. The Managed File Transfer server must be restarted for the changes to take effect.

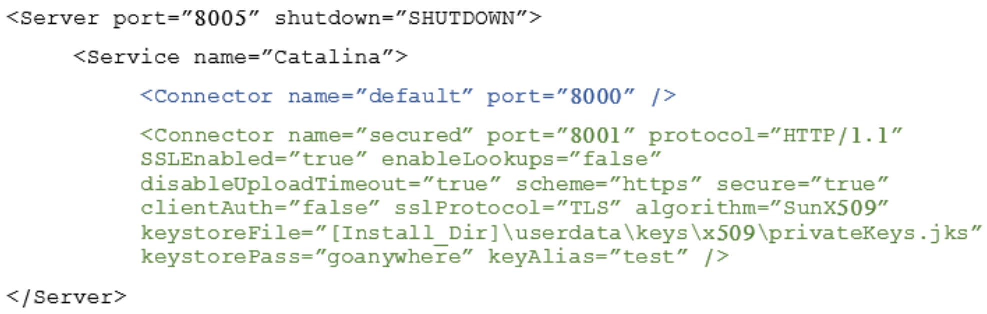
Manually Changing Ports

1. Stop the Managed File Transfer server if it is running.
2. Edit the configuration file `[Install_Dir]/tomcat/conf/server.xml`, where `[Install_Dir]` is the installation directory of Managed File Transfer.
3. Change the port number for the HTTP or HTTPS connectors, for example:
   `<Connector port="8000" />`
4. Change the port number for the shutdown listener, for example:
   `<Server port="8005" shutdown="SHUTDOWN">`
5. Save the configuration file.
6. Start the Managed File Transfer server.

Disabling HTTP or HTTPS Connectors

Managed File Transfer is initially configured to support both HTTP and HTTPS (SSL) connectors for its browser-based Administrator. If you want to disable one of these connectors, then follow the instructions below.

1. Stop the Managed File Transfer server (if it is running).
2. Open the configuration file [Install_Dir]/tomcat/conf/server.xml, where [Install_Dir] is the installation directory for Managed File Transfer.
3. Locate the following XML code:



```
<Server port="8005" shutdown="SHUTDOWN">
     <Service name="Catalina">
          <Connector name="default" port="8000" />
          <Connector name="secured" port="8001" protocol="HTTP/1.1"
          SSLEnabled="true" enableLookups="false"
          disableUploadTimeout="true" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" algorithm="SunX509"
          keystoreFile="[Install_Dir]\userdata\keys\x509\privateKeys.jks"
          keystorePass="goanywhere" keyAlias="test" />
</Server>
```

4. If you do not want to use the HTTP (only use HTTPS) connector, then delete or comment out the line of code illustrated in blue.
5. If you do not want to use the HTTPS (only use HTTP) connector, then delete or comment out the lines of code illustrated in green.
6. If installing to IBM JVM (e.g. IBM i), then set the algorithm="IbmX509"
7. Save the configuration file.
8. Start the Managed File Transfer server.

Note: To comment out XML code, enclose the code with the following indicators:

<!-- to begin the comment
-- to end the comment

Example: <!-- <Connector port="8000" /> -->

SSL (HTTPS) Configuration

A certificate is shipped with Managed File Transfer, which is used (by default) when a user connects to the Managed File Transfer Administrator through their browser over HTTPS. While this default certificate works for establishing a secure channel, users will see warnings about a host name mismatch when they connect. This is because the host name in the shipped certificate will be different than the host name of the machine which you installed Managed File Transfer to.

To avoid these host mismatch warnings, it is recommended to create your own certificate (for your machine's host name) and update the Managed File Transfer configuration file with the new certificate information.

Follow the instructions below to create a new certificate and update the Managed File Transfer configuration file:

1. From within the Managed File Transfer browser-based Administrator, create a new certificate in the Default Private Keys Store. Read the section "Creating a New SSL Certificate" in the on-line help text to learn how to create a certificate. Note that the Common Name in the new certificate must match the domain name, host name, or IP address of the server on which Managed File Transfer is installed.
2. Open the configuration file [Install_Dir]/tomcat/conf/server.xml, where [Install_Dir] is the installation directory for Managed File Transfer. Then modify the value in the keyAlias attribute to be the alias of the new certificate you created in step 1.

Memory Allocation

Managed File Transfer runs in a JVM (Java Virtual Machine) instance, which is allocated 1024 MB of memory by default when the product is installed. This memory is utilized for all features in Managed File Transfer including administration functions and file transfer activity.

Typically 1024 MB of memory is sufficient for most installations. However, if you anticipate high loads (e.g. several thousand file transfers per day), then it is recommended to allocate more memory for the Managed File Transfer JVM. Depending on your operating system, follow the instructions below to change this memory allocation.

Memory Allocation For Windows

1. Navigate to the directory of [Install_Dir]/tomcat/bin, where [Install_Dir] is the installation directory for Managed File Transfer.
2. Find the file named `mft-server.bat`. Right click the file and select to **Run as administrator**.

   Note: This is a service properties program that provides additional information in regards to the JVM being started by the service.
3. Click on the Java tab and edit the Maximum memory pool setting. Specify 2048 for 2GB of memory, 3072 for 3GB of memory, etc…
4. Click on the **Apply** button to save the memory settings.
5. To restart Managed File Transfer for the changes to take effect, click on the General tab and choose to Stop and then Start the service.

Memory Allocation For Unix

1. Navigate to the directory of [Install_Dir]/tomcat/bin, where [Install_Dir] is the installation directory for Managed File Transfer.
2. Edit the file named `mft-server.sh`.
3. Modify the following line in the file:

   ```
   JAVA_OPTS='-Xmx1024m -XX:MaxPermSize=256m -Djava.awt.headless=true'
   ```
4. The setting `-Xmx1024m` is the max memory setting, which is set to 1024 MB by default.

   Change this setting to `Xmx2048m` for 2GB of memory, `-Xmx3072` for 3GB of memory, and so on. Do not change the `MaxPermSize` value. For example:

   ```
   JAVA_OPTS='-Xmx2048m -XX:MaxPermSize=256m -Djava.awt.headless=true'
   ```
5. Save the file.
6. Restart Managed File Transfer for the change to take effect.

Enable Informatica Domain Authentication

If B2B Data Exchange is enabled for Informatica Domain, enable Informatica Security Platform (ISP) authentication for Managed File Transfer before you enable Single Sign On (SSO). After you enable SSO, you can launch Managed File Transfer from the B2B Data Exchange Operation console. Both Managed File Transfer and B2B Data Exchange must be in the same mode for SSO to work, either in native mode or in ISP mode.

1. To launch Managed File Transfer, type the URL on the machine where you installed Managed File Transfer using the format *`https://[hostname]:[https-portnumber]/informaticamft`* or *`http://[hostname]:[http-portnumber]/informaticamft`*.
   - *[hostname]* is the host name or IP address of the Managed File Transfer server
   - *[portnumber]* is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, http://myserver:8000 or https://myserver:8002.
2. Login as an Admin user.
3. From the main menu bar, select **Users**, and then click the **Login Methods** link.
4. For the **Login Method Type** select **Basic Authentication** and click **Continue**.
5. Select **Informatica Domain Authentication** and fill in the following settings:
   - **Name** (required)
   - **Description**
   - Fill in the gateway settings:
     - **Gateway host**: Host name of the Informatica security domain server.
     - **Gateway port number**: Port number for the Informatica security domain gateway. Use the gateway HTTP port number to connect to the domain from the PowerCenter Client. You cannot use the HTTPS port number to connect to the domain.
     - **Username**: User name to access the Administrator tool. You must create the user in the Administrator tool and assign the manage roles/groups/user privilege to the user.
     - **Password**: Password for the Informatica security domain user.

- **Security domain**: Name of the Informatica security domain where the user is defined.

6. Click **Save**.
7. In the Login Methods page, select **Edit**.
8. For the field **Login Methods for Admin Users**, select **Infa-ISP**.
9. Click **Save**.

Creating a Single Sign On Key

Single Sign On (SSO) uses a symmetric key that applications share. When you install Informatica Managed File Transfer, the installation creates a default key and keystore. The key is stored in the keystore, and passphrases protect the key and the keystore. The default passphrase for the key and keystore is `default`. When you generate a master key for SSO, you also create a key generation passphrase known as the keygen passphrase.

Perform the following steps to generate the key on the Managed File Transfer server:

1. To generate a key, run the `mft-keytool.bat` tool in Windows or the `mft-keytool.sh` tool in Linux based systems on the Managed File Transfer server. Run the command with the following syntax:

   ```
   -c generateKey -keygenPassphrase <Key Generation Passphrase> -kp <Key Passphrase> -ksp
   <Key Store Passphrase> -old_kp <Old Key Passphrase> -old_ksp <Old Key Store Passphrase>
   ```

   -c generateKey

   Required. Creates the master key.

   -keygenPassphrase <Key Generation Passphrase>

   Required. Specify a master key passphrase, from 7 to 255 characters, to generate the master key.

   -old_kp <Old Key Passphrase>

   Required. Specify the current passphrase. The default passphrase is `default`.

   -old_ksp <Old Keystore Passphrase>

   Required. Specify the current keystore passphrase. The default passphrase is `default`.

   -kp <Key Passphrase>

   Required. Specify an updated key passphrase, from 7 to 255 characters, that accesses the encryption key.

   -ksp <Keystore Passphrase>

   Required. Specify an updated keystore passphrase from 7 to 255 characters.

2. Stop and restart the Managed File Transfer server.
3. For multiple Managed File Transfer servers in high availability mode, choose one of the following procedures:
   - Generate the key on all the servers using the same keygen passphrase, keystore passphrase, and key passphrase.
   - Alternatively, copy the generated keystore file `keystore.jceks` and the keystore configuration file `sso-security-keystore.properties` from the directory `<MFT_INSTALL_DIR>\mft\config\security` to the same directory on the high availability servers.

To share the master key and enable SSO, install the key on the B2B Data Exchange server. For further information, see the *B2B Data Exchange Installation Guide*

Enable SAML Authentication for Web Users

Security Assertion Mark-Up Language (SAML) is an XML based open standard for authorization and authentication between an Identity Provider and a Service Provider. During authentication, a SAML assertion transfers from Identity Providers to Service Providers. Service Providers use XML statements contained in assertions to make access-control decisions.

You can configure Informatica Managed File Transfer as a Service Provider to authenticate Web Users using an Identity Provider, such as ADFS, OpenAM, Shibboleth, Salesforce.com, SimpleSAMLphp, and more. Managed File Transfer supports SAML v2.0 Web Browser SSO Profile, with HTTP POST and HTTP Redirect bindings. A Web User account must exist before it can be authenticated using SAML. If Managed File Transfer cannot process the SAML assertion, the Web User will be directed to the File Transfer Portal Login page.

Use the following procedure to enable SAML authentication for Web Users.

1. To launch Managed File Transfer, type the URL on the machine where you installed Managed File Transfer using the format `https://[hostname]:[https-portnumber]/informaticamft` or `http://[hostname]:[http-portnumber]/informaticamft`.
   - *[hostname]* is the host name or IP address of the Managed File Transfer server
   - *[portnumber]* is the port number of the Managed File Transfer server. The default port for HTTP is 8000 and the default port for HTTPS is 8002, for example, http://myserver:8000 or https://myserver:8002.
2. Login as an Admin user.
3. To import the certificate, perform the following steps:
   a. From the main menu bar, select **Encryption** and click the **SSL Certificate Manager** link.
   b. Select the **Default Trusted Certificates** key store and click **Open**.
   c. On the toolbar, click **Import Certificate**.
   d. Browse for the certificate file and click **Import**.
   e. Specify an **Alias** to identify the certificate.
4. To create a Private Key to exchange between Managed File Transfer and the SAML provider, perform the following steps:
   a. From the Managed File Transfer main menu bar, select **Encryption** and click the **SSL Certificate Manager** link.
   b. Click **Open Key Store**.
   c. For the **Choose Key Store Type** setting select **Default Private Keys** and then click **Open**.
   d. Fill in the **Key Type**, **Key Size**, **Signature Algorithm**, **Alias**, **Common Name**, and other fields.
5. To create a Web User in Managed File Transfer, perform the following steps:
   a. From the main menu bar, select **Users**, and then click the **Web Users** link.
   b. In the **Web Users** page, click the **Add Web User** link in the page toolbar.
   c. Choose the **Web User Template** to apply security settings for the Web User, and then click **Continue**.
   d. Enter the Web User information.
   e. To add the Web User account, click **Save** .
6. To set the File Transfer Portal preferences in Managed File Transfer, perform the following steps:
   a. From the main menu bar, select **Services** and then click the **Service Manager** link.

b. Select to edit the **HTTPS/AS2** Service.

c. Select **Preference** > **File Transfer Portal**.

d. In the **General** tab, select **Enabled**. For the **Site URL** field enter the IP address, and for the port, use the HTTPS Listener port.

7. To set the SAML preferences, perform the following steps:

a. Select **SAML Single Sign-On**.

b. In the **General** tab, select **Enabled** and **Force Identity Provider Login**.

c. In the **General** tab, you can define the following parameters:

Enabled

Enable SAML Single Sign-On (SSO).

Force Identity Provider Login

When enabled, all authentication requests to the File Transfer Portal must go through the Identity Provider. When disabled, Web Users can authenticate to the File Transfer Portal by accessing the login page URL.

Logout Redirect URL

The alternate URL to forward the Web User to when they log out of the File Transfer Portal. By default, Managed File Transfer directs a Web User to the File Transfer Portal Login page when they log out.

d. In the **Identity Provider** tab, you can define the following parameters:

Entity ID

The ID given to the Identity Provider as the trusted ID. This ID is also used as the expected certificate alias of the Identity Provider's certificate within the default trusted certificates key store.

Binding

Select the type of protocol method for the Identity Provider.

- HTTP POST - Posts a form that contains the message body.
- HTTP Redirect - Sends the message body as query parameters.

Post URL

When the HTTP POST binding is selected, you must enter the URL used to post authentication requests to.

Redirect URL

When the HTTP Redirect binding is selected, you must enter the URL used to send the message body as query parameters.

Server Time Offset

If the Identity Provider and Managed File Transfer system time are not in sync, you can specify a time offset which will be applied to the assertion's time window (in seconds). This is sometimes necessary when the Identity Provider is not within the same network as Managed File Transfer and you cannot control the servers time.

Import Metadata

Managed File Transfer can import the Identity Provider settings, including the Identity Provider certificate, from a SAML Metadata XML file.

1. Click the **Choose File** button and browse to the Metadata file.
2. If the Metadata file contains a certificate, it will be added to the Default Trusted Certificates Key Store using the entity ID as the certificate alias. If the certificates already exists, you can choose Replace Certificate If Exists to overwrite the existing certificate.
3. Click the **Import Metadata** button to parse the Metadata file and populate the Identity Provider settings.

e. In the **Service Provider** tab, specify the following parameters:

Entity ID

The ID given to Managed File Transfer as the trusted ID. Typically this is the host name defined for Managed File Transfer (similar to the Site URL).

Private Store Certificate Alias

The alias of the certificate located in the Default Private Key Store used to sign requests and decrypt assertions. Click the … icon to browse and select the certificate.

Require Signed Response

Determines if Managed File Transfer requires the response to be signed. Typically the response and/or the assertion is signed to establish trust between the Identity Provider and Managed File Transfer.

Require Signed Assertion

Determines if Managed File Transfer requires the assertion to be signed. Typically the response and/or the assertion is signed to establish trust between the Identity Provider and Managed File Transfer.

Require Encrypted Assertion

Determines if Managed File Transfer requires the assertion to be encrypted when it is received. This is typical when SSL is not used for communication between Managed File Transfer and Identity Provider.

f. In the **Username** tab, you can define the following parameters:

Username Location

Select the NameID or Attribute where the user name is found.

NameID

The NameID element.

NameID Format

The format of the NameID element within the SAML response. Managed File Transfer will validate the NameID format before authenticating the SAML assertion. Managed File Transfer supports the following SAML Core V2.0 options:

- Unspecified
- X509SubjectName
- Windows Qualified Domain Name

- Email Address
- Persistent
- Transient
- Kerberos
- Entity

Attribute Name Format

The format of the attribute element that identifies a username within the SAML response. Managed File Transfer will validate the attribute format before authenticating the SAML assertion. Managed File Transfer supports the following SAML Core V2.0 options:

- Basic
- Uniform Resource Identifier

Attribute Name

The attribute name within the assertion XML that identifies the username.

Parse Username Value

When enabled, the value retrieved from the assertion can be parsed using a regular expression pattern.

Username Pattern

Specify a regular expression to parse a user a username value from the attribute.
NameID Example: The x509SubjectName NameID element format for user kharris is 'uid=kharris,ou=marketing,o=example,dc=example,dc=com.' To identify kharris using the uid, use uid=(.*),o=.* for the regular expression.

Attribute Example 2: The username 'kharris' will be parsed from the email address attribute from the SAML assertion. To identify the username, you can use the ([^@]+) regular expression to parse 'kharris' from 'kharris@example.com.'6

Test Response

Allows you to submit a sample assertion response to validate the current configuration.

Base64 Encoded

If the assertion is Base64 encoded, enabling this option will decode the assertion before validating.

SAML Response

Copy your sample assertion to this field.

Validate

Click the Validate button to validate the sample assertion against the SSO settings configured on the SAML tab. Managed File Transfer will attempt to find the user and verify they are authorized for the File Transfer Portal.

Note: It is suggested that you set the global log level to debug while configuring SAML Single Sign-On. The SAML request and response messages will be written to the log, and can be validated using the Test Response option.

g. In the Service Provider tab, click **Export Metadata**.

Managed File Transfer creates a file named `Service Provider.xml`.

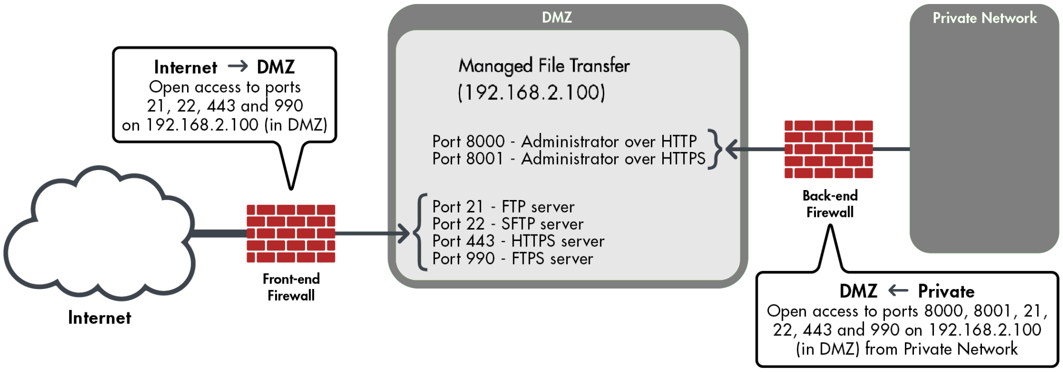
8. On the SAML provider machine, you can add the Service Provider Managed File Transfer, as a relying party in the Identity Provider by importing the metadata file generated in the preceding step.

Firewall Recommendations

If you want to make Managed File Transfer available to external clients over the internet, it is important that you only open certain port numbers to the machine in which Managed File Transfer is installed. This can be controlled through your firewall settings. The firewall settings will depend on whether if the Managed File Transfer software is installed in your DMZ (Demilitarized Zone) or the Private (internal) network, and whether if it is used in conjunction with Managed File Transfer Gateway.

Installation in the DMZ

This diagram illustrates Managed File Transfer as installed in the DMZ.



Internet → DMZ
Open access to ports 21, 22, 443 and 990 on 192.168.2.100 (in DMZ)
DMZ
Managed File Transfer
(192.168.2.100)
Port 8000 - Administrator over HTTP
Port 8001 - Administrator over HTTPS
Port 21 - FTP server
Port 22 - SFTP server
Port 443 - HTTPS server
Port 990 - FTPS server
Private Network
Back-end Firewall
Front-end Firewall
Internet
DMZ ← Private
Open access to ports 8000, 8001, 21, 22, 443 and 990 on 192.168.2.100 (in DMZ) from Private Network

Please note that the IP addresses shown are for demonstration purposes only.

Firewall Configuration

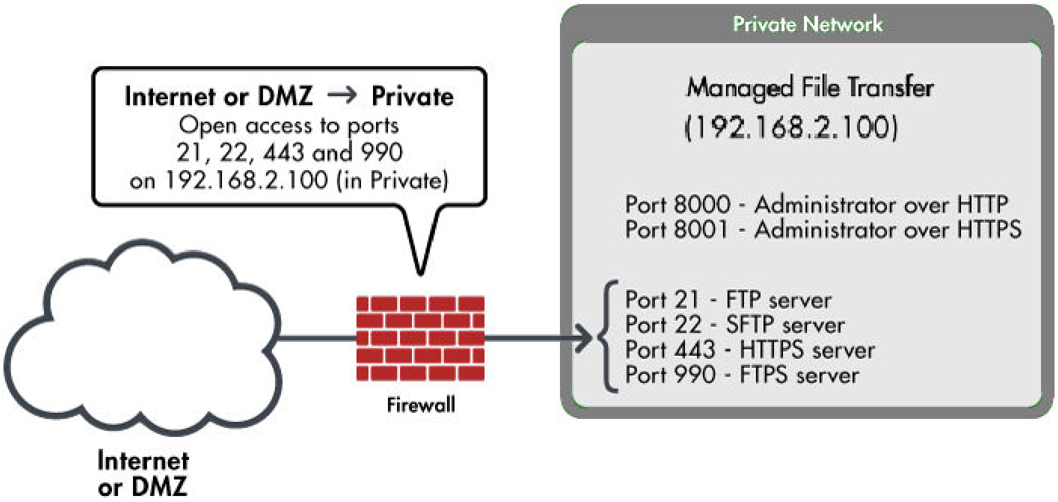
In order to administer Managed File Transfer from any workstations in the private network, ports 8000 and 8002 will need to be opened (through the backend firewall) from the private network to Managed File Transfer in the DMZ.

If external trading partners need access to the file transfer protocols (e.g. SFTP, FTP, HTTPS, AS2, FTPS) in Managed File Transfer, those port numbers (e.g. 21, 22, 443, 990) need to be opened through the frontend firewall to Managed File Transfer in the DMZ. Additionally, if employees (on the private network) need to access those file transfer protocols in Managed File Transfer, the port numbers will need to be opened through the backend firewall from the private network to Managed File Transfer in the DMZ.

If trigger events in Managed File Transfer need to call Remote Projects , then ports 8000 and 8002 need to be opened (through the backend firewall) from Managed File Transfer to another Managed File Transfer server in the private network.

Installation in the Private Network

This diagram illustrates Managed File Transfer as installed in the Private network.



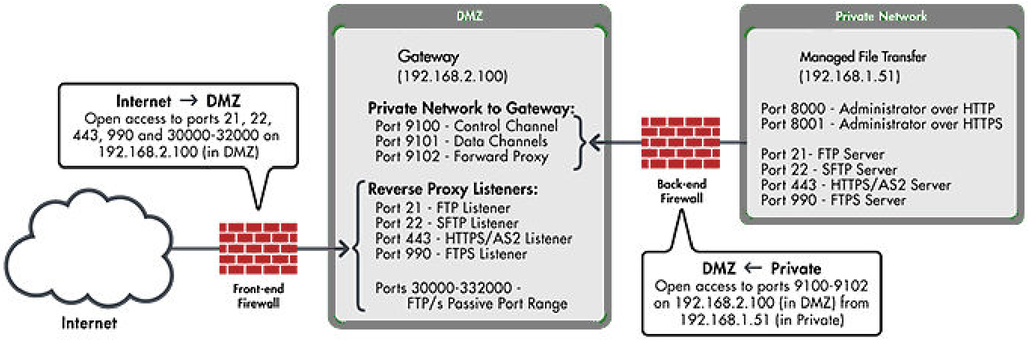
Note: The IP addresses shown are for demonstration purposes only.

Firewall Configuration

If external trading partners need access to the file transfer protocols (e.g. SFTP, FTP, HTTPS, AS2, FTPS) in Managed File Transfer, those port numbers (e.g. 21, 22, 443, 990) need to be opened through the firewall to Managed File Transfer in the private network.

Installation with Managed File Transfer Gateway

This diagram illustrates Managed File Transfer as installed in the Private network, in conjunction with Managed File Transfer Gateway in the DMZ. This configuration allows your organization to keep sensitive files, credentials and logs in the Private network. This configuration also does not require any incoming ports opened into the Private network, which provides a high level of security.


DMZ
Gateway
(192.168.2.100)
Private Network to Gateway:
Port 9100 - Control Channel
Port 9101 - Data Channels
Port 9102 - Forward Proxy
Reverse Proxy Listeners:
Port 21 - FTP Listener
Port 22 - SFTP Listener
Port 443 - HTTPS/AS2 Listener
Port 990 - FTPS Listener
Ports 30000-332000 -
FTP/s Passive Port Range
Private Network
Managed File Transfer
(192.168.1.51)
Port 8000 - Administrator over HTTP
Port 8001 - Administrator over HTTPS
Port 21- FTP Server
Port 22 - SFTP Server
Port 443 - HTTPS/AS2 Server
Port 990 - FTPS Server
Internet → DMZ
Open access to ports 21, 22,
443, 990 and 30000-32000 on
192.168.2.100 (in DMZ)
Front-end
Firewall
Internet
Back-end
Firewall
DMZ ← Private
Open access to ports 9100-9102
on 192.168.2.100 (in DMZ) from
192.168.1.51 (in Private)

Note: The IP addresses shown are for demonstration purposes only.

Firewall configuration:

In order to establish control and data channels from Managed File Transfer to Managed File Transfer Gateway, ports 9100 and 9101 will need to be opened (through the backend firewall) from the Private Network to Managed File Transfer Gateway in the DMZ. Port 9102 will also need to be opened from the Private Network to Managed File Transfer Gateway for Forward Proxy services.

The port numbers (e.g. 21, 22, 443, 990 and 30000-32000) for the desired file transfer protocols (e.g. FTP, SFTP, HTTPS, FTPS, AS2) need to be opened through the frontend firewall to Managed File Transfer Gateway in the DMZ.

Importing a Custom Mass Ingestion Task and Project

Before you can use the custom Informatica Managed File Transfer task and project to run the Data Integration mass ingestion task, import the relevant task and project.

1. Copy the file `MITaskRunner-1.0.jar` from the directory `<MFTInstallationDir>\MFT\server\samples\MI\` to the directory `<MFTInstallationDir>\userdata\lib`.
2. Restart Informatica Managed File Transfer.
3. In the Informatica Managed File Transfer console, select **System** > **Custom Tasks** and click **Install Custom Task**.
4. In the **Install Custom Task** page, for the **Implementation Task**, enter `com.informatica.b2b.mft.RunMITask` and click **Next**.
5. For the name, enter `RunMITask`.
6. Click **Install**. The RunMITask appears as a custom task.
7. Select **Workflows** > **Projects** and select the **DXProjects\<folder>** folder. You must have Write permission if you import to the **DXProjects\Send** folder.
8. Select **Import Projects** > **Import from XML** and
9. Select **Choose File** and select the file `DX_Remote_MI_Send` from the directory `<MFTInstallationDir>\MFT\server\samples\MI\`.
10. Click **Import**. The project DX_Remote_MI_Send appears in the list of available projects.

CHAPTER 5

Product Administration

This chapter includes the following topic:

Starting and Stopping Managed File Transfer

This section contains the procedures to start and stop Managed File Transfer.

Start Managed File Transfer in Windows

Start the Managed File Transfer by following these instructions:

1. Go to the Windows machine and logon with an administrator account.
2. Go to **Control Panel** > **Administrative tools** > **Services**.
3. In the Services window, right-click on Managed File Transfer and select **Start**. After starting Managed File Transfer, its status is updated to **Started**.

Stop Managed File Transfer in Windows

Perform the following steps to stop Managed File Transfer:

1. Login with an administrator account.
2. Go to **Control Panel** > **Administrative tools** > **Services**.
3. In the **Services** window, right-click on the Managed File Transfer and select **Stop**.

Start Managed File Transfer in UNIX

Start the Managed File Transfer by following these instructions:

1. Open a Terminal window.
2. Change the working directory to the tomcat directory where Managed File Transfer is installed, for example `<Managed File Transfer installation>/MFT/server/tomcat/bin`.
3. Start Managed File Transfer by running the following command:
   ```
   mft-server.sh start
   ```

Stop Managed File Transfer in UNIX

Perform the following steps to stop Managed File Transfer:

1. Open a Terminal window.
2. Change the working directory to the directory where Managed File Transfer is installed.
3. Stop the Managed File Transfer by executing the running the following command:
   ```
   mft-server.sh stop
   ```

CHAPTER 6

Upgrade Overview

You can upgrade the following versions of Managed File Transfer directly to the latest version:

- Managed File Transfer version 10.2.3
- Managed File Transfer version 10.2.2 HF1
- Managed File Transfer version 10.2.2

Note: To perform a silent upgrade of Managed File Transfer , refer to “Installing Managed File Transfer on a Silent Mode” on page 16

Upgrading Managed File Transfer on Windows

Perform the following steps to upgrade the Managed File Transfer product on a Windows machine.

1. Login to the target Windows system as an administrator.
2. Stop Managed File Transfer.
3. Download the Managed File Transfer installer `Install.exe` file.
4. Execute the downloaded `Install.exe` file and follow the prompts on the screens to upgrade Managed File Transfer.
5. To start the Managed File Transfer application server perform the following instructions:
    a. Go to **Control Panel** > **Administrative tools** > **Services**.
    b. In the Services window, right-click on **Informatica MFT 10.2.3** and select **Start**.
    c. Within seconds after starting Managed File Transfer, its status should be updated to “Started”. If not, contact Informatica Support.

Note: Managed File Transfer is configured in Windows as an automatic startup Service. This means that the Managed File Transfer will automatically start whenever Windows starts.

Upgrading Managed File Transfer on UNIX

Perform the following steps to upgrade Managed File Transfer onto a UNIX server.

1. Create or designate a non-root user on the system that will be used to install and run the Managed File Transfer application. This user will be the owner of all files created during installation as well as files written to the file system during use.

2. Login to the server.
3. Download the Managed File Transfer UNIX installer `Install.bin` file.
4. Open a Terminal window.
5. Change the directory to where the installer file was downloaded.
6. Run the installer.
7. Follow the on-screen instructions to complete the upgrade.
8. Start the Managed File Transfer by following these instructions:
    1. Open a Terminal window.
    2. Change the working directory to the tomcat directory at the path where Managed File Transfer is installed, for example `Opt/Informatica/B2B/MFT/server/tomcat/bin`.
    3. Start the Managed File Transfer by executing the following shell script: `./mft-server.sh` start.
9. The installation and startup of Managed File Transfer is complete.

CHAPTER 7

Active-Passive: Backups and Replication

Follow the instructions in this section if you are using Managed File Transfer in an Active-Passive, non-clustered configuration, in which only one installation of Managed File Transfer will run at a time. Follow the instructions for an Active-Active setup if you will run Managed File Transfer in a clustered environment. For more information about the Active-Active setup, see Chapter 8, "Active-Active: Clustering and Automatic Failover" on page 40.

Backing Up Managed File Transfer User Data

All user data and configurations for Managed File Transfer are stored in a directory called `userdata`, which is located under the Managed File Transfer installation directory.

The default paths to the `userdata` folder for each platform is listed below:

- Windows: `C:\Informatica\B2B\MFT\server\userdata`
- UNIX: `/usr/local/Informatica/B2B/MFT/server/userdata`

Important: You should backup the Managed File Transfer `userdata` folder (and its contents) in your regular backup processes. It is recommended to backup the `userdata` folder at least daily.

Replicating Managed File Transfer User Data for High Availability

Managed File Transfer user data can be replicated to another system for high availability and failover purposes. Managed File Transfer does not have a built-in replication function, so you will need to use a separate tool to replicate the necessary data to the high availability machine.

Setting Up Replication

Follow these steps to set up replication:

1. Install Managed File Transfer onto the high availability machine using the regular installation method.

2. Test the Managed File Transfer installation on the high availability machine to make sure it works properly.
3. Shut down the Managed File Transfer subsystem/service on the high availability machine, since Managed File Transfer should not be running on both the production and high availability machines at the same time.
4. Set up your high availability tool to replicate the directory named `userdata`, which is located under the Managed File Transfer installation directory on the production machine. The `userdata` directory contains all user data and configurations for Managed File Transfer. Make sure to include all the subdirectories under the `userdata` directory, except do not replicate the subdirectory named `/userdata/database/mft/` since there will be a lock on that subdirectory while Managed File Transfer is running. This subdirectory contains the embedded database, which is saved nightly (by default) to the subdirectory named `userdata/database/backups`.

Setting Up Failover

The steps to follow in order to run Managed File Transfer on the high availability machine depends on if your production machine is still up-and-running.

If your production machine is down and you want to switch to the high availability machine:

1. Start the Managed File Transfer subsystem/service on the high availability machine.

   If your production machine is running and you want to switch to the high availability machine, perform the following steps
2. Perform a backup of the Managed File Transfer database using your usual backup method.
3. Shut down the Managed File Transfer subsystem/service on the production machine.
4. Copy the backup of the database from the production machine into the `/userdata/database/mft` directory on the high availability machine.
5. Start the Managed File Transfer subsystem/service on the high availability machine.

CHAPTER 8

Active-Active: Clustering and Automatic Failover

Clustering allows two or more Managed File Transfer installations (systems) to work together to provide file transfer services for the enterprise. This provides greater scalability by allowing workloads to be distributed horizontally across multiple Managed File Transfer systems.

If one Managed File Transfer system fails, the remaining systems in the cluster will automatically continue to process workloads and file transfer requests.

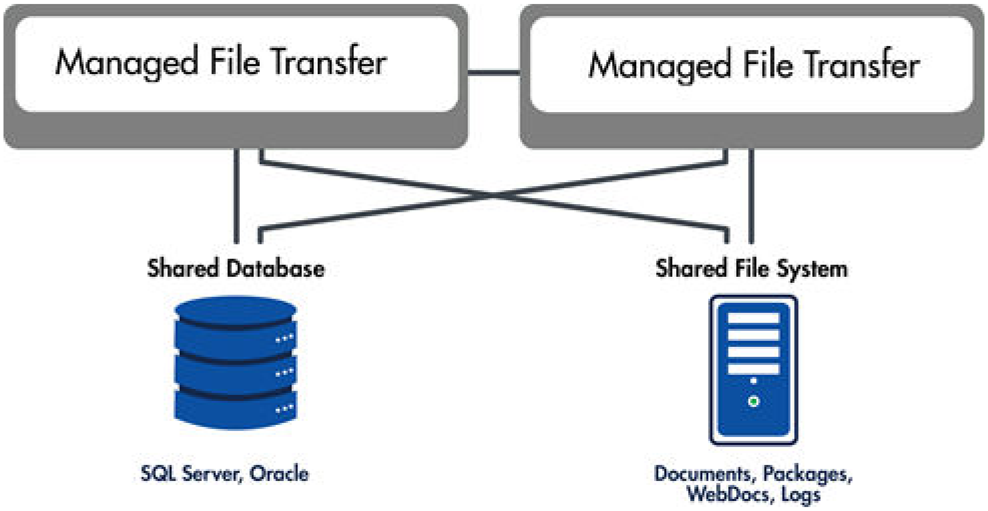
This active-active clustered environment also provides the best high availability option for handling potential system failures. If one Managed File Transfer system fails, the remaining systems in the cluster will automatically continue to service the trading partners.

The following features are available in Managed File Transfer when running in a cluster:

- Two or more Managed File Transfer systems within a cluster can connect to the same external database at the same time. This allows these systems to share security settings, trading partner user accounts, configurations, audit logs and other product tables. The database can be configured or switched from any system in the cluster, in which the new database settings will be replicated to all systems in the cluster.
- The System Name (specified in [InstallationDirectory]/config/cluster.xml) for each participant in the cluster will appear on the Managed File Transfer login screen, on the top-right corner of the dashboard and any cluster-related screens. This name will also be recorded in audit log records to indicate which system was servicing a trading partner's session during each event. The system name is accessible in Triggers using the event.systemName variable.
- The Active Sessions screen displays all trading partner sessions (IP address, user name, login date, audit activity) for any system in the cluster. Within this screen, sessions can also be terminated (killed) on any system in the cluster.
- Managed File Transfer Gateway configurations can be viewed, updated, started and stopped from any Managed File Transfer system within the cluster.
- Auto blacklist features for "Denial of Service" and "Brute Force" attacks are cluster-aware. This allows each Managed File Transfer system (in the cluster) to share security activity with each other to determine when to block attacking IP addresses from the cluster.
- The Max Sessions setting for a Web User account will limit the total number of that user's sessions for all systems within the cluster. For instance, if the Max Sessions for a Web user is set to 2 and if they are logged into 2 different systems in the cluster, then they will not be able to open any additional sessions in the cluster at that time.

When setting up a cluster, you will need to install Managed File Transfer onto two or more servers. It is recommended that the Operating Systems and JRE versions on these servers to be the same for simplifying configuration.

The following diagram illustrates two instances of Managed File Transfer in a cluster, in which both instances are using a shared database and file system.



Setting up the First System in the Cluster

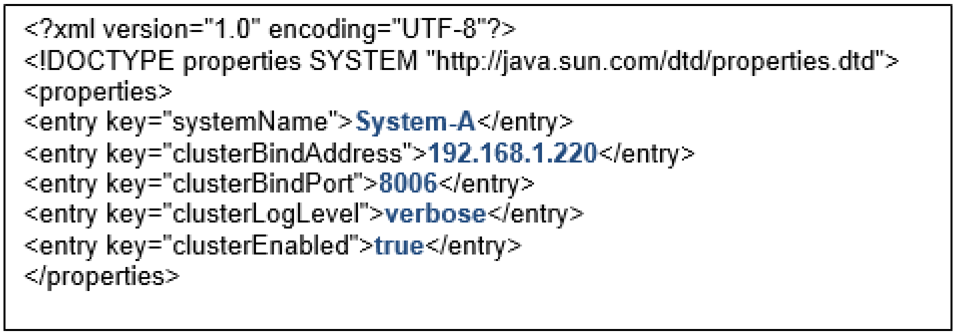
To configure the first system in the cluster, perform the following steps.

1. Start Managed File Transfer and login to the browser-based Administrator.
2. All systems in the cluster are required to use the same external database (SQL Server or Oracle in network mode). The Switch Database wizard located in the **System** > **Database Configuration** section will guide you through the process to utilize an external database. Data in the existing database can be automatically migrated to the new external database.
3. All systems in the cluster must point to the same set of shared folders for storing documents, certificates and other user files. It is recommended that these folder paths are pointing to a shared network location. Follow the steps below:
   a. Navigate to the **System** > **Global Settings** page. On the **Data** tab, specify the shared network folders for each feature.
   b. Navigate to the **Logs** > **Log Settings** page and configure the Logs Directory to point to a shared network folder.
   c. Navigate to the **Services** > **Shared Drive Settings** page and configure Shared Drive Directory to point to a shared network folder.
   d. If Web Users need to authenticate using digital certificates for HTTPS or FTPS protocols, then the locations of the SSL Key Stores should point to a shared network location that all systems in the cluster have access to. To specify the Key Store locations select **Encryption** from the main menu and choose the **SSL Certificate Manager** option, and then select **Preferences**. Specify the shared network locations for the key stores on the Default Trusted Certificates and Default Private Keys.
4. After the configuration is completed in the steps above, verify that there are no active sessions on this installation. Then you should shut down the Managed File Transfer service or subsystem.

5. Go to the file system of the server that Managed File Transfer is installed on and open the file named `[InstallationDirectory]/config/cluster.xml`, where [InstallationDirectory] is the location that Managed File Transfer is installed to. The following properties need to be configured in this file:

   - **systemName** - A unique name to identify this system in the cluster. The maximum system name length is 20 characters.
   - **clusterBindAddress** - The IP address which Managed File Transfer will listen on to communicate with other Managed File Transfer systems in a cluster. This IP address must be valid on this server which Managed File Transfer is installed to.
   - **clusterBindPort** - The port number which Managed File Transfer will listen on to communicate with other Managed File Transfer systems in a cluster. For example, 8006.
   - **clusterLogLevel** - The log level of “info” will record all standard log messages from each system in the cluster. When the log level is set to “verbose” the log will also record all of the system-to-system messages used to manage the cluster. While initially testing clustering within your environment, it is recommended to keep the log level at “verbose” to get more detailed messages.
   - **clusterEnabled** - This must be set to “true”.

   The following image shows an example of `cluster.xml` file.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="systemName">System-A</entry>
<entry key="clusterBindAddress">192.168.1.220</entry>
<entry key="clusterBindPort">8006</entry>
<entry key="clusterLogLevel">verbose</entry>
<entry key="clusterEnabled">true</entry>
</properties>
```

6. After configuring `cluster.xml`, you can restart Managed File Transfer.

   This system will assume the coordinator role since it is the first Managed File Transfer system started in the cluster.

7. Review the Managed File Transfer global log for any errors. Sign into the Administrator and navigate to **Logs** > **Server Log Viewer**. The log file is named `informatica_<systemName>.log`, where `systemName` is the unique name to identify this system in the cluster that was specified previously.

Setting up Additional Participant Systems in the Cluster

Perform the following steps to configure each additional participant system in the cluster.

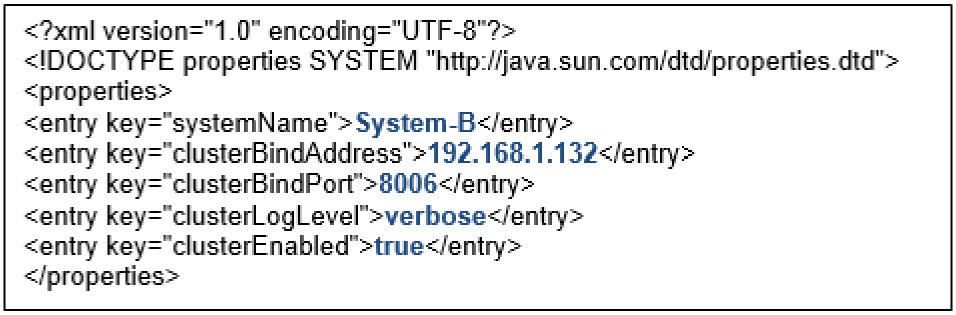
1. Start Managed File Transfer and login to its browser-based Administrator.
2. Select **Server** > **Database Configuration** > **Switch Database**. Follow the steps to switch this database over to the same database that the first system in the cluster uses.

   Important: On Step 5 of the Switch Database process, select **Do Nothing, the database already has valid tables, indexes and data**.

3. Verify that there are no active sessions on this installation. After that, shut down Managed File Transfer on the participant system.
4. Configure the `cluster.xml` file for this system with the instructions in the procedure to setting up the first system in the cluster. Ensure to specify a unique system name and IP for this installation.

   The following image shows the `cluster.xml` file.

   Figure 1.

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
   <properties>
   <entry key="systemName">System-B</entry>
   <entry key="clusterBindAddress">192.168.1.132</entry>
   <entry key="clusterBindPort">8006</entry>
   <entry key="clusterLogLevel">verbose</entry>
   <entry key="clusterEnabled">true</entry>
   </properties>
   ```

5. After configuring `cluster.xml`, you can restart Managed File Transfer.

   This system is a participant since it was not the first Managed File Transfer system started in the cluster.

6. Review the Managed File Transfer global log for any errors. Sign into the Administrator and navigate to **Logs** > **Server Log Viewer**. The log file will be named `informatica_systemName.log`.

Troubleshooting Errors

The following items identify problems that may occur when a Participant attempts to join a cluster:

1. If you receive an error about product versions not matching, then the Participant is running a different version of Managed File Transfer than the Coordinator system. All systems in the cluster must be running on the same Managed File Transfer version.
2. If you receive an error about the timestamp on the Participant not being within five minutes of the Coordinator system, then you must change the system clock on the Participant system to be in sync with the Coordinator. The time is compared in UTC and ignores time zone differences.
3. You may receive an error about one of the documents directories not being shared. This can occur when the Coordinator system can access the directory but a Participant cannot. In this case you will need to log in to the Coordinator system and configure the Logs, Packages, WebDocs or Documents directories to ensure they are the accessible for all systems in the cluster.
4. You may receive an error about how the Participant system shut down because another system is actively using the database. This can occur when the Participant and Coordinator systems cannot connect to each other over the clustering communications channel. It is important that the Coordinator's IP and port (used for the communications channel) is accessible by the other Participant systems. If that address is blocked by a firewall or other network restrictions, then this system will not be considered as part of the cluster and will be forced to shut down.

Clustering Failover

Managed File Transfer executes several background processes to purge records, send notifications and to perform other housekeeping processes. This processing is the responsibility of the Coordinator system. If the Coordinator system becomes unresponsive, then the next Participant to join the cluster will become the Coordinator.

For example, if a cluster was started with three systems (System-A, System-B and System-C) in that order, then System-A will be the Coordinator since it was the first to join the cluster. If System-A fails for any reason, then System-B will become the new Coordinator. If System-A is restarted and successfully rejoins the cluster, then the order of the systems (for becoming a Coordinator) would then be System-B, System-C and then System-A. If System-B were to crash, then System-C would become the new Coordinator.

It is possible for the clustering communications channel between the systems to break due to network interruptions or other reasons. Managed File Transfer has built-in heartbeats and other safety checks to overcome small network interruptions. However, if the communication becomes unresponsive for 60 seconds, then the Participant systems will believe that the Coordinator system has failed. When that happens, each Participant will start checking the database to see if the Coordinator system is still running.

If the Coordinator system is still running after 30 seconds (if the communications channel fails) then the Participant systems will automatically shut down. This is required in order to prevent issues that can occur when multiple Managed File Transfer systems are running on the same database and not communicating with each other. In this rare scenario, even though the Participant systems were shut down, the Coordinator system will still be up and running.

Backups

When Managed File Transfer is running in a clustered environment, the following items are recommended to be backed up on a regular and automated basis:

1. The external database that Managed File Transfer is running on. Speak with your database administrator to make sure this database is part of the backup process.
2. The folder locations for the Logs, Packages, Documents and WebDocs directories. Speak with your network administrator to make sure that these locations are part of the backup process.
3. All user data and configurations for Managed File Transfer are stored in the [InstallationDirectory]/userdata folder. Although the Logs, Packages and other directories should be pointing to network locations it is still recommended to make backups of this location for custom email templates, SSL certificates and other files that are not using a network location.

CHAPTER 9

Uninstalling Managed File Transfer

This section describes how to uninstall the Managed File Transfer product.

Caution: All Managed File Transfer configurations, resources and project definitions will be deleted during the uninstall process.

Uninstall from Windows

Perform the following steps to uninstall Managed File Transfer from Windows:

1. Stop the Managed File Transfer on the Windows system.
2. Browse to the installation directory of Managed File Transfer.
3. Run the file named `uninstall.exe`.

Uninstall from UNIX

Perform the following steps to uninstall Managed File Transfer from UNIX:

1. Verify that no jobs are currently running in the Managed File Transfer Administrator.
2. Change the working directory to the directory where Managed File Transfer was installed .
3. Stop the Managed File Transfer by running the following command:
   ```
   ./mft-server.sh stop
   ```
4. Uninstall the Managed File Transfer product by executing the following command: `./uninstall`

INDEX