Informatica

Informatica® B2B Data Exchange
10.2.3

Managed File Transfer Gateway Guide

Informatica B2B Data Exchange Managed File Transfer Gateway Guide
10.2.3
February 2019

Publication Date: 2020-05-21

Table of Contents

Preface

Follow the instructions in the *Managed File Transfer Gateway Guide* to install and configure Managed File Transfer Gateway. Learn how to administer Managed File Transfer Gateway in addition to pre- and post-requisite tasks.

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.

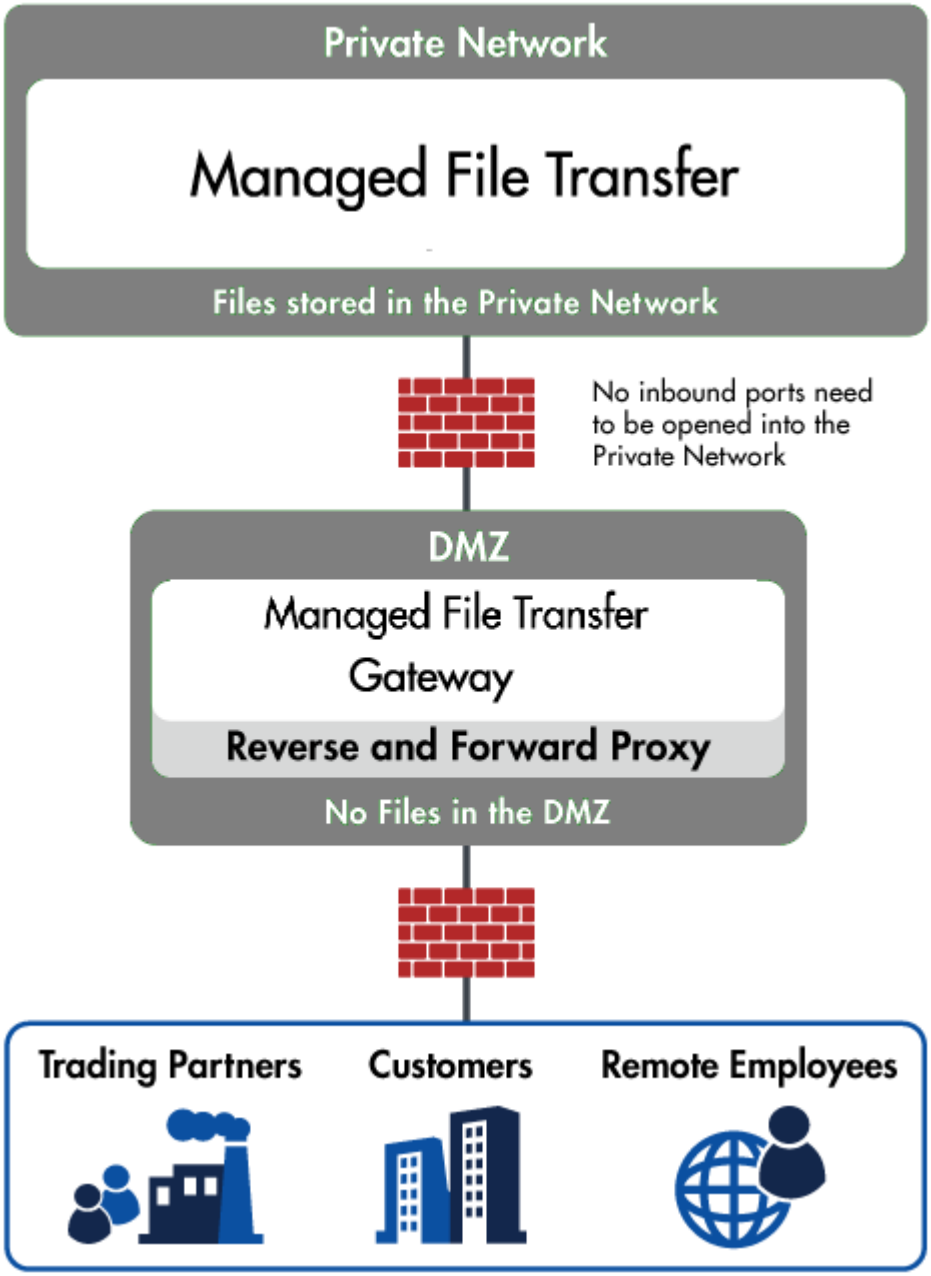
CHAPTER 1

Introduction

Managed File Transfer Gateway is both an enhanced reverse proxy and forward proxy. It provides an additional layer of network security when your organization needs to safely exchange data with your trading partners. When using Managed File Transfer Gateway as a reverse proxy, no inbound ports need to be opened into the private/internal network and no sensitive data needs to be stored in the demilitarized zone (DMZ).

Managed File Transfer Gateway is a software-only solution which is installed in the DMZ or public-facing network. Trading Partners only connect to authorized ports on Managed File Transfer Gateway, which routes requests over a proprietary channel to back-end services (for example, FTP, SFTP, HTTP Server) in the private/internal network. This approach allows your organization to keep sensitive information (for example, data files, user credentials, keys, certificates) in the private/internal network, keeping your DMZ in compliance.

When Managed File Transfer Gateway is used as a forward proxy for outbound connections, it will hide the identities and locations of those internal systems. In essence, Managed File Transfer Gateway serves as a transparent interface between internal systems and external systems without exposing sensitive files and the private/internal network. This is an essential solution for meeting strict security policies and complying with state privacy laws, HIPAA, PCI DSS, SOX, ISO 27000 and GLBA.



Managed File Transfer Gateway offers the following features and benefits:

- No incoming ports need to be opened into the private/internal network- reduces the risk of network intrusion
- No sensitive data files need to be stored in the DMZ
- No user credentials, permissions, certificates and keys need to be stored in the DMZ
- Hides the locations and identities of internal systems
- Service configurations are maintained/stored in the private network
- Supports FTP, FTPS, SFTP, SCP, HTTP, HTTPS and AS2 file transfer protocols
- Built-in load balancer to distribute workloads across multiple systems

- No special hardware components required; software-only solution
- Installs to Windows, Linux, AIX, UNIX and Solaris operating systems

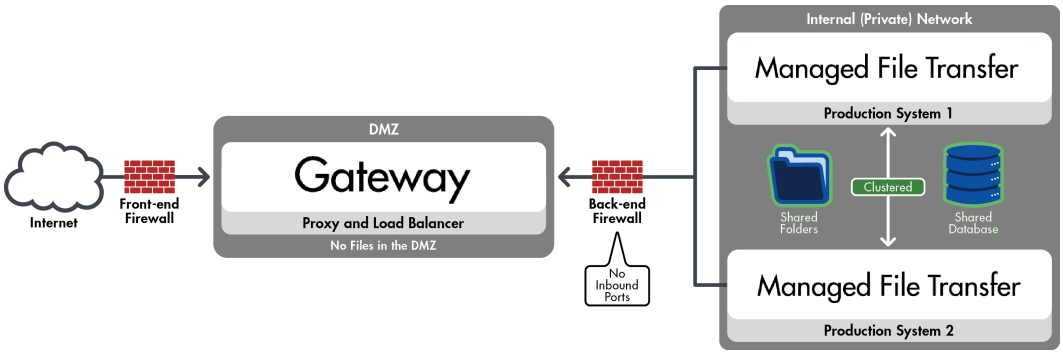
How Does it Work?

Managed File Transfer Gateway can serve as both a Reverse Proxy and a Forward Proxy. Typically Managed File Transfer Gateway is installed in the demilitarized zone (DMZ) and is installed in the private/internal network.

At startup, creates an outbound connection to Managed File Transfer Gateway, which is used as a "control channel" for passing commands and messages between the products. This control channel will initially provide the proxy details (IP and port mappings) to Managed File Transfer Gateway, at which point it will start up "listeners" on the designated IPs and ports for incoming traffic.

Reverse Proxy

When an external client (trading partner) connects to a listener on Managed File Transfer Gateway in the DMZ, Managed File Transfer Gateway will make a request over the control channel to in the private/internal network. will then create a new outbound data channel to Managed File Transfer Gateway. This data channel will be attached to the desired service (for example, FTP, FTPS, SFTP, HTTP/s) and all traffic for that session will be routed over this new data channel including client authentication requests, data and commands. When the session is terminated, the corresponding data channel will be removed.



Forward Proxy

The Forward Proxy in Managed File Transfer Gateway allows you to route client requests from (in the internal network) to external FTP, FTPS, SFTP and SCP servers without revealing the identity or locations of your internal systems. The Forward Proxy is additionally used by to route active and passive FTP and FTPS data connections through Managed File Transfer Gateway.

When a process in needs to make an outbound connection through the proxy, a request is made to Managed File Transfer Gateway with the address of the intended destination. Managed File Transfer Gateway will then establish the connection to that destination and will bridge it to the requesting system.

CHAPTER 2

Installing Managed File Transfer Gateway

The following sections describe how to install Managed File Transfer Gateway on the supported platforms.

System Requirements

Managed File Transfer Gateway installs to all popular enterprise server operating systems. Listed below are the supported operating systems and minimum hardware/software requirements for installing Managed File Transfer Gateway.

Windows	
Disk Space Usage	400 MB
Minimum Memory	256 MB
Java Runtime Environment (JRE)	1.8.0.77 or higher must be installed prior to the installation.

Linux and Solaris	
Disk Space Usage	400 MB
Minimum Memory	256 MB
Java Runtime Environment (JRE)	1.8.0.77 or higher must be installed prior to the installation.

AIX	
Disk Space Usage	50 MB
Minimum Memory	256 MB
Java Runtime Environment (JRE)	1.8 SR2 FP10 must be installed prior to the installation.

Installing Managed File Transfer Gateway on Windows

Perform the following steps to install Managed File Transfer Gateway on Windows 64-bit operating systems. The installer creates a Windows Service that starts automatically when the system is booted.

1. Launch the installation wizard by double clicking on the `Install.exe` installer file.
2. Select to install the Managed File Transfer Gateway. Follow the on-screen instructions to complete the installation.

   Note: During installation, you will be prompted to specify options such as IP addresses and port numbers. For more information, see "Server Configuration" on page 18.
3. To start the Gateway, see Chapter 3, "Administering Managed File Transfer Gateway" on page 13.
4. To configure Managed File Transfer to work with Managed File Transfer Gateway, refer to the *Managed File Transfer User Guide*.

Installing Managed File Transfer Gateway on UNIX

Perform the following steps to install Managed File Transfer Gateway on UNIX based operating systems.

1. Open a Terminal window.
2. Change the working directory to the directory where the installer file was downloaded by running the `cd` command (for example, `cd [installer_directory]`)
3. Launch the installer by typing the command `Install.bin -i console`.
4. Select to install the Managed File Transfer Gateway. Follow the on-screen instructions to complete the installation.

   Note: During installation, you will be prompted to specify options such as IP addresses and port numbers. For more information, see "Server Configuration" on page 18.
5. To start the Gateway, see Chapter 3, "Administering Managed File Transfer Gateway" on page 13.
6. To configure Managed File Transfer to work with Managed File Transfer Gateway, refer to the *Managed File Transfer User Guide*.

CHAPTER 3

Administering Managed File Transfer Gateway

The topics in this section provide instructions for administering Managed File Transfer Gateway, such as starting and stopping the Gateway and other commands.

Starting Managed File Transfer Gateway

The instructions for starting Managed File Transfer Gateway depends on the operating system. Perform the steps in the appropriate section to start Managed File Transfer Gateway.

Start the Windows Service

1. Log in to the target Windows system where Managed File Transfer Gateway is installed.
2. Open the **Services** window from the Control Panel.
3. Right-click the service named **Informatica MFT Gateway 10.1.0** in the **Services** window.
4. Click **Start** from the context menu.

Start the Service on Linux or UNIX

1. Log in to the target Linux or UNIX system where Managed File Transfer Gateway is installed.
2. Open a Terminal window.
3. Execute the command `/opt/Informatica/B2B/MFT/gateway/bin/mft-gateway.sh start`.

Stopping Managed File Transfer Gateway

The instructions for stopping Managed File Transfer Gateway depends on the operating system. Perform the steps in the appropriate section to stop Managed File Transfer Gateway.

Stopping the Windows Service

1. Log in to the target Windows system where Managed File Transfer Gateway is installed.
2. Open the **Services** window from the Windows Control Panel.
3. Right-click the service **Informatica MFT Gateway 10.1.0** in the **Services** window and select **Stop** the context menu.

Stopping the Linux or UNIX Service

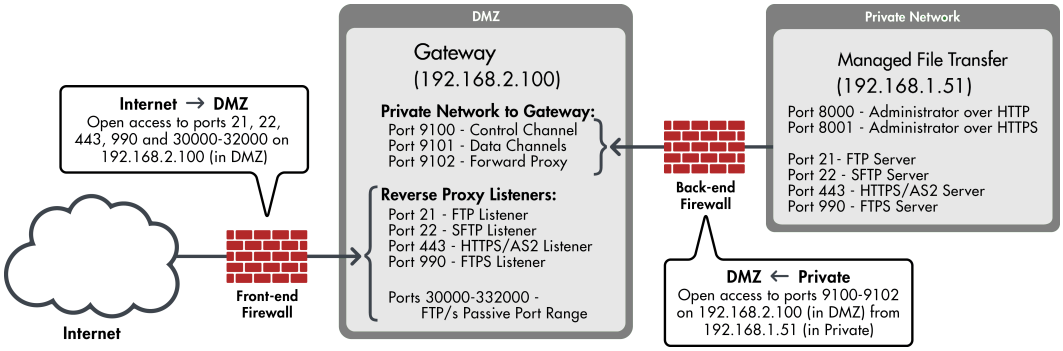
1. Log in to the target Linux/UNIX system where Managed File Transfer Gateway is installed.
2. Open a Terminal window.
3. Run the command `/opt/Informatica/B2B/MFT/gateway/bin/mft-gateway.sh stop`.

CHAPTER 4

Firewall Configuration

In order to provide protection for sensitive files and the private (internal) network, Managed File Transfer Gateway should be installed in the DMZ and should be installed in the private network. The frontend and backend firewalls should be configured to open only specific port numbers to the products.

The diagram below shows the firewall settings if the default port numbers were used in Managed File Transfer Gateway and Managed File Transfer. The IP addresses shown are for demonstration purposes only.



Frontend Firewall Configuration

The following table shows the standard port numbers for the desired file transfer protocols that need to be opened through the frontend firewall to Managed File Transfer Gateway in the DMZ:

Port	Description
21	FTP
22	SFTP
443	HTTPS
990	FTPS
30000-32000	Must be opened to support passive mode for FTP or FTPS.

Backend Firewall Configuration

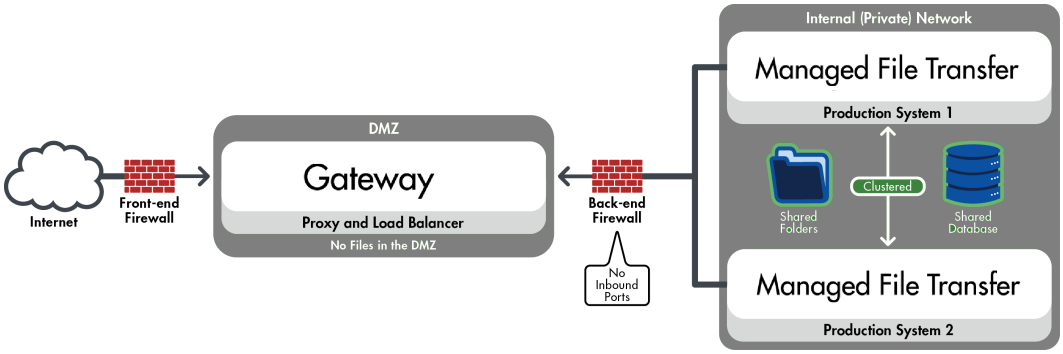
In order to establish control and data channels from to Managed File Transfer Gateway, the following ports must be opened through the backend firewall from the Private Network to Managed File Transfer Gateway in the DMZ:

Port	Usage
9100	Outbound connection to the Managed File Transfer Gateway control connection listener. This is used for the persistent control connection between and Managed File Transfer Gateway.
9101	Outbound data connection that is used to handle client connections from the protocol listeners (FTP, SFTP, HTTPS, FTPS, AS2) in . A connection is made from to this port for each client connection.
9102	Used for the Forward Proxy services. For more information, see "How Does it Work?" on page 10.

CHAPTER 5

Load Balancing

Managed File Transfer Gateway can serve as a load balancer for distributing workloads across multiple installations within a cluster. This active-active framework provides greater high availability for mission-critical environments.



As a load balancer, Managed File Transfer Gateway spreads connections evenly across the clustered systems. This load balancing algorithm is called “round-robin”, which is a common load balancing standard.

FTP, FTPS and SFTP are stateful protocols and use the round robin algorithm to load balance connections across the systems in the cluster.

HTTP/S is a stateless protocol which also uses the round robin algorithm, however it needs to persist each connection (for a period of time) to the same HTTP/S server in order to maintain the integrity of the session. This is important because the user’s HTTP/S session is typically only able to be serviced by a single HTTP/S server at a time.

The configuration settings for the round-robin load balancing rules are located in the gateway.xml file (found in the installation folder). For new installations, the `gateway.xml` file already has the rules provided for load balancing with in a clustered environment. Prior installations of Managed File Transfer Gateway (that upgrade to version 2.0.0) will need to add the Load Balancing rules to the `gateway.xml` file.

CHAPTER 6

Configuring Managed File Transfer Gateway

Managed File Transfer Gateway's configuration can be customized by editing the configuration files located in `[install_directory]/gateway/`. The files in this directory are XML files, which can be edited with any text or XML editor. The following configuration files can be edited:

gateway.xml

Contains the basic configuration options such as the IP addresses and port number that Managed File Transfer Gateway should use.

log4j.xml

Contains the options for customizing the logs generated by Managed File Transfer Gateway. With this configuration file, you can control the level of logging, redirect the logs to a Syslog server, etc.

Server Configuration

To configure the Managed File Transfer Gateway server, open the `gateway.xml` file located in the `[install_directory]/gateway/` directory using a text or XML editor.

Listed below are the attributes that can be updated:

Attribute Name	Description
controllerAddress	The local IP address on which Managed File Transfer Gateway should listen for Control Connections from . Be sure this IP address is reachable from the system where is installed.
controllerPort	The port number on which Managed File Transfer Gateway should listen for Control Connections from Managed File Transfer. The default port number is 9100. Be sure this port is open for outbound connections on the firewall protecting the private network.
dataAddress	The local IP address on which Managed File Transfer Gateway should listen for Data Connections from Managed File Transfer. When an external client connects to the Managed File Transfer Gateway, opens a data connection which attaches to the desired service. The IP address specified here should be accessible from the system where is installed.

Attribute Name	Description
dataNATAddress	The IP Address that should connect to when establishing a data connection with Managed File Transfer Gateway. Managed File Transfer Gateway will send this address to when a new client connects. This should be used only if connections from to Managed File Transfer Gateway are routed through a NAT firewall.
dataPort	The port number on which Managed File Transfer Gateway should listen for Data Connections from Managed File Transfer. The default port number is 9101. Be sure to open this port for outbound connections on the firewall protecting the private network.
dataNATPort	The port number Managed File Transfer Gateway will direct to connect to when establishing a data connection. This should be used only if connections from to Managed File Transfer Gateway are routed through a NAT firewall.
forwardProxyLocalAddress	The local IP address Managed File Transfer Gateway will use when active data connections are requested. This address is also used to establish outbound connections to remote servers when Managed File Transfer Gateway is used as a forward proxy. The value should be the local IP you wish to have used when establishing an outbound connection from the Managed File Transfer Gateway server.
proxyAddress	The local IP address on which the Outbound Proxy component of Managed File Transfer Gateway should listen for incoming requests. The Outbound Proxy works similar to a SOCKS Proxy, which accepts CONNECT and BIND requests from clients. A CONNECT request is used to connect out to another system on the Internet, whereas the BIND request is used to temporarily listen on a port for accepting incoming connections from a system on the Internet. The Outbound Proxy is used by the FTP and FTPS services in to facilitate routing of passive and active data connections through the Managed File Transfer Gateway. When an external FTP client requests a data connection in passive mode, the FTP service sends a BIND request to the Outbound Proxy. Managed File Transfer Gateway then listens on a temporary port for the incoming connection. After accepting the connection, any data is routed to the intended destination. When an external FTP client requests an active data connection, the FTP service sends a CONNECT request to the Outbound Proxy specifying the IP address and port it should connect to. Once the connection is established, any data will be routed to the intended destination. The Outbound Proxy can also be used by when using the FTP, FTPS, SFTP and SCP protocols.
proxyNATAddress	The IP Address that should connect back to when establishing an FTP Active or Passive data connection through Managed File Transfer Gateway. Managed File Transfer Gateway will send this address to during the initial handshake, and will connect to this address when an FTP/S client requests an Active or Passive data connection (see proxyAddress). This should be used only if you are supporting FTP/S Active or Passive data connections in , and if all connections from to Managed File Transfer Gateway are routed through a NAT firewall. This is not required when using Managed File Transfer Gateway as a forward proxy from .
proxyPort	The port number on which the Outbound Proxy component of Managed File Transfer Gateway should listen for incoming connections. The default port number is 9102. Be sure to open this port for outbound connections on the firewall protecting the private network.

Attribute Name	Description
proxyNATPort	The port number which Managed File Transfer Gateway will direct to connect to when establishing an FTP Active or Passive data connection through Managed File Transfer Gateway. Managed File Transfer Gateway will send this port to during the initial handshake, and will connect to this port when an FTP/S client requests an Active or Passive data connection (see proxyPort). This should be used only if you are supporting FTP/S Active or Passive data connections in , and if all connections from to Managed File Transfer Gateway are routed through a NAT firewall. This is not required when using Managed File Transfer Gateway as a forward proxy from .
passiveProxyAddress	The local IP address on which the Managed File Transfer Gateway should listen for incoming passive FTP data connections from external clients.
passiveProxyPortRangeFrom	The beginning port in the range of ports available for FTP passive data connections.
passiveProxyPortRangeTo	The ending port in the range of ports available for FTP passive data connections.
proxyEnabled	The outbound proxy component of Managed File Transfer Gateway can be enabled or disabled.
shutdownPort	The port number on which Managed File Transfer Gateway should listen for shutdown requests. For security reasons, Managed File Transfer Gateway binds the shutdown listener on the LOOPBACK address, thus ensuring shutdown requests are accepted only from the local host. The default port number is 9105.
minThreads	The minimum number of spare threads that Managed File Transfer Gateway should always have available. The default value is 10.
maxThreads	The maximum number of threads that Managed File Transfer Gateway is allowed to use. The default value is 2000.
threadKeepAlive	The number of seconds an unused thread would stay alive before it is discarded. The default value is 60 seconds.

Note: Managed File Transfer Gateway must be restarted for any changes to take effect. If the controllerAddress or controllerPort have changed, all instances of that are setup to use this gateway must also be updated, and the connection to Managed File Transfer Gateway must be restarted.

Load Balancer

The following attributes can be defined for each load balancing rule:

Rule

Attribute	Description
name	A unique name that identifies the load balancer rule. The Managed File Transfer Gateway configuration specified in will use this name when defining the load balancing option for a particular service. Use the recommended name of **default** for stateful protocols like FTP, FTPS and SFTP. Use the name **https** for stateless protocols like HTTP/S.

Load Balancer

Attribute	Description
algorithm	The load balancer algorithm to use for the rule. The supported algorithm is **roundrobin**.

Session Persistence

Attribute	Description
type	For stateless protocols, like HTTPS, sessions must be persisted based on IP addresses. The valid value is **ip**.
timeout	When using Session Persistence, this setting determines the expiration of a persisted session. This time is specified in seconds and should be equal to or greater than the session timeout specified for the HTTPS service in . Connections received from the same IP address before the timeout will be routed to the same system as the previous connection. The timeout is also reset each time a connection is made from the same IP address.

Default gateway.xml Configuration

The server configuration file that is shipped with Managed File Transfer Gateway contains the following settings:

```
<?xml version="1.0" encoding="UTF-8"?>
<gateway controllerAddress="192.168.1.212" controllerPort="9100"
dataAddress="192.168.1.212" dataPort="9101" shutdownPort="9105"
proxyEnabled="true" proxyAddress="192.168.1.212"
proxyPort="9102"
passiveProxyAddress="192.168.1.212"
passiveProxyPortRangeFrom="30000"
passiveProxyPortRangeTo="32000"
forwardProxyLocalAddress="192.168.1.212"
minThreads="10" maxThreads="2000" threadKeepAlive="60">
<rules>
<rule name="default">
<loadBalancer algorithm="roundrobin" />
</rule>
<rule name="https">
<loadBalancer algorithm="roundrobin">
<sessionPersistence type="ip" timeout="300" />
</loadBalancer>
</rule>
</rules>
</gateway>
```

Logging Configuration

To update the logging configuration, edit the `log4j.xml` file located in the `[install_directory]/gateway/config/` directory. By default, logs are written to a file named `infa-mft-gateway.log`, located in the `[install_directory]/gateway/logs` directory. Managed File Transfer Gateway can also send messages to an enterprise Syslog server. To change the file logging settings, edit one or more parameters in the

<appender name="FileAppender"> section of the configuration file. The following table describes logging parameters:

Attribute Name	Description
File	The file to which logs are written. The value can either be an absolute path or relative to the installation directory. Escape any backslashes used in the path by adding another backslash (e.g. C:\\logs\\infagateway.log).
MaxFileSize	The maximum size that the log file is allowed to reach before being rolled over to backup files. The value must be a whole number, followed by KB, MB or GB to represent Kilobytes, Megabytes and Gigabytes respectively.
MaxBackupIndex	The maximum number of retained backup files. When the backup files reach the specified limit, the oldest backup is deleted. The value must be a whole number. If set to zero, no backup files are created.

Syslog Logging Configuration

By default Syslog logging is disabled. You can enable Syslog logging by un-commenting the sections in blue. To un-comment, remove the <!-- and --> around the <appender name="SyslogAppender"> sections. The following table contains the parameters that can be adjusted for Syslog logging:

Attribute Name	Description
Protocol	The protocol used for dispatching log messages to the Syslog server. Valid values are - UDP and TCP.
SyslogHost	The host name or IP address of the Syslog server.
Facility	The Syslog facility name to which messages are logged. Valid values are - KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6 and LOCAL7.
Ident	The application ID you would like to assign to the messages that are sent to the Syslog server. The default value is infagateway.
CharSet	Specify the character set to use for encoding the log messages. The default value is UTF-8, which works well for all character data.

Log Level Configuration

The type of messages logged by Managed File Transfer Gateway can be adjusted by changing the log level. The default log level is info, which logs important informational messages along with any warnings and errors. The supported log levels are:

Error

Logs only the error messages

Warn

Logs all errors and warning messages

Info

Logs all errors, warnings and important informational messages

Debug

Logs all above messages along with additional debug level messages

Trace

Logs all above messages along with the tracing of data that is sent or received

Note: To change the log level, update the line `<level value="info" />` to the desired level. Setting the level to `Debug` or `Trace` may degrade the performance of Managed File Transfer Gateway under high load.

Changes made to the configuration file requires restarting of Managed File Transfer Gateway to take effect.

Default log4j.xml Configuration

The logging configuration file that is shipped with Managed File Transfer Gateway contains the following settings.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/" debug="false">
<appender name="FileAppender" class="org.apache.log4j.RollingFileAppender">
<param name="File" value="logs/gagateway.log" />
<param name="MaxFileSize" value="5MB" />
<param name="MaxBackupIndex" value="10" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="%d{yyyy-MM-dd hh:mm:ss a} %-5p %m%n" />
</layout>
</appender>
<!--
<appender name="SyslogAppender"
class="org.productivity.java.syslog4j.impl.log4j.Syslog4jAppender">
<param name="Protocol" value="udp" />
<param name="Facility" value="user" />
<param name="SyslogHost" value="localhost" />
<param name="Ident" value="gagateway" />
<param name="CharSet" value="utf-8" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="%-5p %m" />
</layout>
</appender>
-->
<logger name="com.linoma.gag" additivity="false">
<level value="info" />
<appender-ref ref="FileAppender" />
<!--
<appender-ref ref="SyslogAppender" />
-->
</logger>
<root>
<level value="error" />
<appender-ref ref="FileAppender" />
</root>
</log4j:configuration>
```

The comments in the file are excluded.

The `<appender name="FileAppender">....</appender>` and `<appender-ref ref="FileAppender">...</appender-ref>` sections are used for file logging.

The `<appender name="SyslogAppender">...</appender>` and `<appender-ref ref="SyslogAppender">...</appender-ref>` sections are used for Syslog logging. Syslog logging is disabled by default.

Backup and Recovery

Managed File Transfer Gateway configuration and log data can be replicated to another system for high availability and failover purposes. Managed File Transfer Gateway 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.

Configuring Replication

To set up replication, perform the following steps.

1. Install Managed File Transfer Gateway onto the high availability machine using the regular installation method.
2. Test the Managed File Transfer Gateway installation on the high availability machine to make sure it works properly.
3. Shut down the Managed File Transfer Gateway service on the high availability machine, since Managed File Transfer Gateway 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 Gateway installation directory on the production machine. The `userdata` directory contains all user data and configurations for Managed File Transfer Gateway. Make sure to include all the subdirectories under the `userdata` directory, except do not replicate the subdirectory named `/userdata/database/services/` since there is a lock on that subdirectory while Managed File Transfer Gateway is running. This subdirectory contains the embedded database, which is saved nightly by default to the subdirectory named `userdata/database/backups`.

Configuring Failover

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

1. If your production machine is down and you want to switch to the high availability machine, perform the following steps:
   a. On the high availability machine, copy the latest backup of the Managed File Transfer Gateway database from the subdirectory named `userdata/database/backups` into the subdirectory named `/userdata/database/services`. The database is as up-to-date as the last time the database was backed up on the production machine.
   b. Start the Managed File Transfer service on the high availability machine.
2. If your production machine is running and you want to switch to the high availability machine, perform the following steps:
   a. Perform a backup of the Managed File Transfer Gateway database.
   b. Shut down the Managed File Transfer Gateway service on the production machine.
   c. Copy the backup of the database from the production machine into the `/userdata/database/services` directory on the high availability machine.
   d. Start the Managed File Transfer Gateway service on the high availability machine.

Backups

When Informatica MFT Gateway is running in a clustered environment, the following items are recommended to be backed up on a regular and automated basis:

- All user data and configurations for Informatica MFT Gateway 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 7

Uninstalling Managed File Transfer Gateway

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

Uninstalling from Windows

To uninstall all Managed File Transfer products from Windows, perform the following steps.

1. Stop the Managed File Transfer service on the Windows system.
2. Browse to the installation directory of Managed File Transfer Gateway and run the file named `uninstall.exe` to uninstall all Managed File Transfer products.

Uninstalling from UNIX

To uninstall Managed File Transfer Gateway from UNIX, perform the following steps.

1. Change the working directory to the directory where Managed File Transfer Gateway is installed.
2. Stop Managed File Transfer Gateway by running the following command: `/opt/Informatica/B2B/MFT/gateway/bin/mft-gateway.sh stop`.
3. Uninstall the Managed File Transfer Gateway product by running the following shell script: `./uninstall.sh`.