Control-M Managed File Transfer
9.0.19.100
Setup Guide

July 2019
Contacting BMC Software

You can access the BMC Software website at http://www.bmc.com. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

Address  
BMC SOFTWARE INC  
2103 CITYWEST BLVD  
HOUSTON TX  
77042-2827  
USA

Telephone  
• 713 918 8800  
• 800 841 2031

Fax  
713 918 8000

Outside United States and Canada

Telephone  
(01) 713 918 8800

Fax  
(01) 713 918 8000

© Copyright 1999-2018 BMC Software, Inc.

Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of BMC Software, Inc.

BMC, BMC Software, the BMC logo, the BMC Software logo, and other BMC marks, and the tagline “Bring IT to Life” are the exclusive properties of BMC Software, Inc., or its affiliates or subsidiaries and are registered or may be registered with the U.S. Patent and Trademark Office and in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

For BMC Control-M Products that are licensed on the “per CPU – Full Capacity” unit of measurement and installed in an Amazon Web Services (“AWS”), Microsoft Azure (“Azure”), or Google Cloud Platform (“GCP”) cloud environment, a license is required for the total number of CPUs in each AWS, Azure, or GCP instance upon which the Product is installed or which the Product manages, either remotely or locally. For AWS and GCP, one CPU is equivalent to one vCPU, as defined by AWS. For Azure, one CPU is equivalent to up to four Virtual Cores (as defined by Azure), rounded up to the closest multiple of four.

Server Endpoint Licensing

All machines upon which any Control-M component is installed or upon which Control-M managed workload runs must be licensed. This includes Control-M Agent/Agentless platforms onto which one or more application plug-ins are installed but also includes Control-M Agent/Agentless platforms where no application plug-ins are installed. Control-M Agent/Agentless platforms on which jobs are ordered are counted regardless of whether those jobs execute or not. All Server Endpoints are counted, including development, staging, QA, pre-production, test, and production environments.

The licensing guidelines for application plug-ins are as follows:
• ERP and BI/DI: The application server(s) upon which Control-M managed processes are executed should be licensed in addition to the Control-M Agent machine(s) (in some cases, this may be the same machine).

• Databases: Each database server upon which Control-M managed database related processes are being executed should be counted in addition to the Control-M Agent machine(s).

• AFT and MFT: Only the machine(s) upon which the AFT or MFT plug-in is installed should be licensed.

• Web Services, Java & Messaging: only the Control-M Agent machine(s) upon which the plug-in is installed should be licensed.

• Backup: The Control-M Agent machine(s) where the Backup plug-in is installed and also the hosts which are running the backup server software should be licensed (note that this excludes the client machines for which the Backup Server software is managing actual backup processes except where a backup takes place of the backup server machine itself).

• Cloud: only the Control-M Agent machine(s) upon which the plug-in is installed should be licensed.

• Hadoop: All machines in each managed Hadoop Cluster should be licensed.

IBM® Tivoli® Business Service Manager, IBM Tivoli Workload Scheduler, IBM Cognos, IBM InfoSphere DataStage, IBM i (AS/400), IBM WebSphere, and AIX® are the trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

UNIX® is the registered trademark of The Open Group in the US and other countries.

Linux is the registered trademark of Linus Torvalds.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

SAP® R/2 and SAP R/3, SAP Business Objects, and SAP NetWeaver are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Restricted rights legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Field 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.

Customer support

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

Support website

You can obtain technical support from BMC 24 hours a day, 7 days a week at (http://www.bmc.com/support). From this website, you can:
- Read overviews about support services and programs that BMC offers
- Find the most current information about BMC products
- Search a database for issues similar to yours and possible solutions
- Order or download product documentation
- Download products and maintenance
- Report an issue or ask a question
- Subscribe to receive proactive e-mail alerts when new product notices are released
- Find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

**Support by telephone or e-mail**

In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

**Before contacting BMC**

Have the following information available so that Customer Support can begin working on your issue immediately:

- **Product information**
  - Product name
  - Product version (release number)
  - License number and password (trial or permanent)
- **Operating system and environment information**
  - Machine type
  - Operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - System hardware configuration
  - Serial numbers
  - Related software (database, application, and communication) including type, version, and service pack or maintenance level
- **Sequence of events leading to the issue**
- **Commands and options that you used**
- **Messages received (and the time and date that you received them)**
  - Product error messages
  - Messages from the operating system, such as file system full
  - Messages from related software
License key and password information
If you have questions about your license key or password, contact BMC as follows:

- (USA or Canada) Contact the Order Services Password Team at 800 841 2031, or send an e-mail message to ContractsPasswordAdministration@bmc.com.
- (Europe, the Middle East, and Africa) Fax your questions to EMEA Contracts Administration at +31 20 354 8702, or send an e-mail message to password@bmc.com.
- (Asia-Pacific) Contact your BMC sales representative or your local BMC office.

Third party Software
For the provisions described in the BMC License Agreement and Order related to third party products or technologies included in the BMC Product, see https://docs.bmc.com/docs/display/workloadautomation/Control-M+Workload+Automation+Documentation and click Third-party software (TPS).
Contents

Control-M Managed File Transfer Setup ...............................................................................................7
Control-M Managed File Transfer installation .....................................................................................7
Deploying Control-M MFT ....................................................................................................................9
Rolling back Control-M MFT ..............................................................................................................11
Configuring the File Transfer Server ..................................................................................................11
Control-M MFT Enterprise B2B ...........................................................................................................17
Control-M Managed File Transfer Setup

Control-M Managed File Transfer (MFT) is an FTP/SFTP client and server solution that enables you to watch and transfer files from a local host to a remote host, a remote host to a local host, or a remote host to another remote host. You can also monitor and track the traffic load, file status, and active connections of all file transfers in Control-M.

To set up Control-M MFT, you need to do the following:

- Install Control-M/EM 9.0.19 or higher, as described in Control-M/EM 9.0.19 Release Notes.
- Install Control-M/Server 9.0.19 or higher, as described in the Control-M 9.0.19 Release Notes.
- Install Control-M Managed File Transfer, as described in Control-M Managed File Transfer installation (on page 7).
- Deploy and update Control-M MFT on your Control-M Agents from the CCM, as described in Deploying Control-M MFT (on page 9).
- Configure a built-in File Transfer Server that supports FTP/S and SFTP protocols with Windows, PAM or LDAP authentication, as described in Configuring the File Transfer Server (on page 11).
- Transfer files between internal Control-M users and external business partners, as described in Control-M MFT Enterprise B2B (on page 17).

Control-M Managed File Transfer installation

The following procedures describe how to install Control-M Managed File Transfer (MFT) on a Control-M/EM server on UNIX and Windows:

- Installing Control-M MFT on Windows (on page 7)
- Installing Control-M MFT on UNIX (on page 8)

The installation copies the MFT packages repository for each OS to EM_HOME/Client_Updates. The packages are used to deploy MFT to multiple Control-M/Agents, as described in Deploying Control-M MFT (on page 9).

Installing Control-M MFT on Windows

This procedure describes how to install Control-M MFT on a Control-M/EM server on Windows.
Before you begin

- Ensure that the database server that contains the Control-M/EM database is up and running.
- Download the MFT installation files (see Product Distribution in the Control-M Managed File Transfer Release Notes).

To install MFT on Windows:

1. From the Control-M MFT Deployment Package CD, double-click the setup.exe file.

   The Control-M Managed File Transfer Deployment Package 9.0.19 wizard appears.

2. Do one of the following:
   - **Interactive install**: Follow the on-screen instructions until the installation is complete.
   - **Automatic install**: Create a parameter file and then run the automatic install in a non-interactive mode, as follows:
     a. Follow the on-screen instructions until the Summary window.
     b. Click Generate and select the location to create the XML parameter file.
     c. Click Yes to quit the installation.
        A confirmation message appears.
     d. Click Yes.
     e. Copy the automatic installation parameters file to a network location that is accessible to all computers where you want to perform an automatic installation.
     f. Log in using a user ID that has Administrator permissions on the current computer.
     g. Ensure that the installation DVD is still in the DVD drive, and run the installation script, as follows:
        `<source_path>\Setup.exe -silent <xml_path>\<filename.xml>`
        The installation log can be found at the following location:
        `<installFolder>\BMCINSTALL\log\BMC_Control-M_Managed_File_Transfer_Install_<date-time>.log`

3. Click Done.

Installing Control-M MFT on UNIX

This procedure describes how to install Control-M MFT on a Control-M/EM server on UNIX.

Before you begin

- Ensure that the database server that contains the Control-M/EM database is up and running.
- Download the MFT installation files (see Product Distribution in the Control-M Managed File Transfer Release Notes).

To install MFT on UNIX:

1. Mount the installation CD from the root user and log off the root user before continuing with the installation.
2. Log in to the Control-M/EM account.
   
   **NOTE:** If you are using the GUI, set the environment variable `DISPLAY` to value `<hostName>:0.0`. It is not necessary to set `DISPLAY` for console mode or silent mode. (For more information, see Setting environment variables in UNIX.)

3. Type the following command:
   
   `<cdPath>/setup.sh`

4. Follow the on-screen instructions until the installation is complete.

**Uninstalling Control-M MFT from Windows**

This procedure describes how to uninstall Control-M MFT from Windows.

➢ To uninstall MFT from Windows:
   
   1. From the **Start** menu, select **Control Panel**.
   2. Double-click **Programs and Features**.
   3. Select **Control-M Managed File Transfer Deployment Package 9.0.19**, and click **Uninstall**.
   4. Click **OK** to continue.

   Control-M MFT is successfully removed from your computer.

**Uninstalling Control-M MFT from UNIX**

This procedure describes how to uninstall Control-M MFT from UNIX.

➢ To uninstall MFT from UNIX:
   
   1. Log in as a Control-M user.
   2. Navigate to the following directory:
      
      `<InstallFolder>/BMCINSTALL/uninstall/DRAFP.9.0.19`
   3. Type one of the following commands:
      
      • Interactive uninstall: `./uninstall.sh`
      • Automatic uninstall: `./uninstall.sh -silent`

   Control-M MFT is successfully removed from your computer.

**Deploying Control-M MFT**

This procedure describes how to transfer MFT installation packages to existing Control-M/Agents and install or upgrade Control-M MFT on UNIX or Windows.
NOTE: You can only deploy MFT 9.0.19 on Control-M for AFT 8.2.00 and higher or Control-M MFT 9.0.00 and higher.

NOTE: You can only deploy MFT 9.0.19 to Control-M/Agent 9.0.18.

NOTE: You cannot upgrade more than one MFT activity on the same Windows computer simultaneously.

➢ To deploy Control-M MFT:

1. From the Manage tab, select Deployment.
   The Deployment window appears.
2. Click New Activity > Managed File Transfer > Install/Upgrade.
   The MFT Upgrade/Install window appears.
3. Do the following:
   a. In the Activity Name field, type a name for this activity.
   b. In the Description field, describe the purpose of this activity (optional).
   c. In the E-Mail Notification Address field, type the email address(es) that you want to receive notifications about this activity (optional).
      To receive email notification, you need to define the email server parameters, as described in SMTP parameters.
4. Select one of the following:
   • Send MFT to Control-M Agent(s): Transfers the MFT installation package to specific Control-M/Agent computers. After the package is transferred, you can manually start the upgrade process, at any time, from the Agent Deployment window or upgrade with CLI, as described in ccmcli.
   • Send and Install MFT to Control-M Agent(s): Transfers the MFT installation package to specific Control-M/Agent computers and begins the upgrade process automatically.

NOTES:

- The Control-M MFT installation package is deleted after a successful upgrade. If the upgrade failed, then the installation package remains on the Control-M/Agent computer until the next successful upgrade.
- The MFT installation package remains on the Control-M/Server computer for 30 days. If you want to change this setting, define the Control-M/Server AD_RETAIN_PACKAGES, as described in Defining Control-M/Server system parameters.

5. Click Next.
6. Select the Control-M/Agent(s) to deploy Control-M MFT.

   NOTE: If you selected a Control-M/Agent on Windows that is set to Logon as User, you need to define the Run As User for each Control-M/Agent.
7. Depending on which method you selected, click Transfer or Upgrade.
The transfer process starts, and progress messages appear in the right pane of the deployment activity. To view and troubleshoot the internal stages of the upgrade, click Log from the Agent Deployment window. If you selected to transfer the installation package, you can upgrade or install Control-M MFT any time after the transfer is complete. A job runs on the Control-M/Agent(s) to verify that it upgraded successfully.

Rolling back Control-M MFT

This procedure describes how to roll back Control-M MFT from multiple Control-M/Agents. You can only roll back Control-M MFT if it was upgraded with the Deployment tool.

This procedure must be done within a defined period based on the AD_GA_RETAIN_DAYS system parameter, as described in Control-M/Agent deployment parameters.

Before you begin

- Verify that all jobs on the selected Control-M/Agents have ended. If jobs are still running during the rollback, they might fail.

➢ To roll back Control-M MFT:

1. From the Manage tab, select Deployment.
   The Deployment window appears.

2. Click New Activity > Manage File Transfer > Rollback.
   The MFT Rollback window appears.

3. Do the following:
   a. In the Activity Name field, type a name for this activity.
   b. In the Description field, describe the purpose of this activity (optional).
   c. In the E-Mail Notification Address field, type the email address(es) that you want to receive notifications about this activity (optional).
   To receive email notification, you need to define the email server parameters, as described in SMTP parameters.

4. Click Next.

5. Select the Control-M/Agent(s) with Control-M MFT to roll back.

6. Click Rollback.
   The rollback process begins immediately and Control-M MFT is removed from the Control-M/Agent. To view and troubleshoot the internal stages of the rollback, click Log from the Deployment window.

Configuring the File Transfer Server

This procedure describes how to configure the File Transfer Server in the CCM, which enables you to transfer files directly from one MFT host to another MFT host, without using an FTP server on a third computer. The File Transfer Server is included on every Control-M/Agent that has Control-M MFT installed, supports both FTP/S and SFTP, and is embedded in the MFT process.
To configure the File Transfer Server:

1. From the CCM, select Control-M Managed File Transfer on the host that you want to manage, right-click and select File Transfer Server.

   The File Transfer Server window appears.

2. Configure the following File Transfer server parameters:
   - File Transfer Server general parameters (on page 13)
   - FTP/FTPS server parameters (on page 14)
   - SFTP server parameters (on page 15)
   - File Transfer Server Authentication parameters (on page 16)

3. Click Save.

4. Restart the File Transfer Server by running one of the following commands:
   - UNIX: cm/AFT/exe/startb2b.sh
   - Windows: cm\AFT\exe\startb2b.sh
File Transfer Server general parameters

The following table describes File Transfer Server general parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Defines the hostname where the File Transfer Server is installed</td>
</tr>
<tr>
<td>Home directory</td>
<td>Defines the root path where transferred files are stored.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you want to use a different directory for each logged in user, you must add <code>\${userName}</code> to the path.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>: <code>C:\temp\${userName}</code></td>
</tr>
<tr>
<td></td>
<td>Bob connects to the File Transfer Server and uploads the file <code>a.txt</code> to the root directory, the file is saved in <code>C:\temp\Bob\a.txt</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: <code>&lt;Agent_Home&gt;/CM/AFT/ftshome/${userName}</code></td>
</tr>
<tr>
<td>Multiple login allowed</td>
<td>Determines whether multiple users can connect to the File Transfer Server simultaneously</td>
</tr>
<tr>
<td>Max. logins</td>
<td>Determines the number of users that can connect to the File Transfer Server simultaneously</td>
</tr>
<tr>
<td>Max login failures</td>
<td>Determines the maximum number of login attempts before a timeout</td>
</tr>
<tr>
<td>Delay between failed login attempts</td>
<td>Determines the number of seconds to wait after a login failure before the next attempt</td>
</tr>
<tr>
<td>Throttling activated</td>
<td>Determines whether to limit number of simultaneous uploads and downloads.</td>
</tr>
<tr>
<td>Max simultaneous uploads</td>
<td>Determines the maximum number of simultaneous uploads</td>
</tr>
<tr>
<td>Max simultaneous downloads</td>
<td>Determines the maximum number of simultaneous downloads</td>
</tr>
</tbody>
</table>
FTP/FTPS server parameters

The following table describes FTP/FTPS server parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable server</td>
<td>Determine whether the File Transfer Server that supports client connection with the FTP/FTPS protocol is enabled</td>
</tr>
<tr>
<td>Port</td>
<td>Determines the port number that the embedded File Transfer Server listens to for FTP/FTPS connections</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: This port is used by clients to connect to the FTP/FTPS server (Default: 1221).</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authenticates the FTP user with one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>- Windows local user</td>
</tr>
<tr>
<td></td>
<td>- LDAP</td>
</tr>
<tr>
<td></td>
<td>- PAM (<em>UNIX only</em>)</td>
</tr>
<tr>
<td>Secured</td>
<td>Determines whether FTP is enabled</td>
</tr>
<tr>
<td>Keystore file path</td>
<td>Defines the path to the file that contains the server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The keystore must be in <strong>PKCS#12</strong> format. If FIPS is enabled, the format must be <strong>BCFKS</strong>.</td>
</tr>
<tr>
<td>Keystore file password</td>
<td>Defines the password of the file that contains the server certificate</td>
</tr>
<tr>
<td>Ciphers</td>
<td>Determines the cipher security settings used for FTP</td>
</tr>
<tr>
<td>Listen for implicit connections</td>
<td>Determines whether to automatically turn on security after a connection is established between the FTPS client and the Managed File Transfer server.</td>
</tr>
<tr>
<td>Passive Port/s:</td>
<td>Limits the range of dynamic ports that can be used for passive connections in FTP. Ports can be defined as single ports, closed or open ranges. Multiple definitions must be separated by commas.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>:</td>
</tr>
<tr>
<td></td>
<td>2300 : Uses 2300 as the passive port</td>
</tr>
<tr>
<td></td>
<td>2300-2399: Uses all ports in the range</td>
</tr>
<tr>
<td></td>
<td>2300-: Uses all ports larger than 2300</td>
</tr>
<tr>
<td></td>
<td>2300, 2305, 2400-: Uses 2300 or 2305 or any port larger than 2400</td>
</tr>
</tbody>
</table>
SFTP server parameters

The following table describes SFTP server parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable server</td>
<td>Determines whether the File Transfer Server that supports client connection with SFTP is enabled</td>
</tr>
<tr>
<td>Port</td>
<td>Determines the port number that the embedded File Transfer Server listens to for SFTP connections</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This port is used by clients to connect to the SFTP server (Default: 1222).</td>
<td></td>
</tr>
<tr>
<td>Keystore file path</td>
<td>Defines the path to the file that contains the client's certificate</td>
</tr>
<tr>
<td>Keystore file password</td>
<td>Defines the password for the file that contains the server's certificate.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The keystore must be in <strong>PKCS#12</strong> format. If FIPS is enabled, the format must be <strong>BCFKS</strong>.</td>
<td></td>
</tr>
<tr>
<td>Ciphers</td>
<td>Determines the cipher security settings used for SFTP</td>
</tr>
<tr>
<td>Known user file path</td>
<td>Defines the path to the file that contains known users by SFTP</td>
</tr>
<tr>
<td>Authentication</td>
<td>Authenticates the FTP user with one of the following methods:</td>
</tr>
<tr>
<td></td>
<td>▪ Windows local user</td>
</tr>
<tr>
<td></td>
<td>▪ LDAP</td>
</tr>
<tr>
<td></td>
<td>▪ PAM (<strong>UNIX only</strong>)</td>
</tr>
<tr>
<td>Override home directory for specific internal users</td>
<td>Determines which internal users can override their specific home directory to connect to the FTS/Hub with SFTP. The home directory changes are saved in the <strong>fts_config.properties</strong> file in the following format:</td>
</tr>
<tr>
<td></td>
<td><strong>home.directory.expression.&lt;user&gt;==&lt;home_dir&gt;</strong></td>
</tr>
<tr>
<td><strong>NOTE:</strong> The home directory can be a network path in the UNC format.</td>
<td></td>
</tr>
</tbody>
</table>
File Transfer Server Authentication parameters

The following table describes LDAP Authentication parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search user</td>
<td>Defines the LDAP Browse user</td>
</tr>
<tr>
<td>Password</td>
<td>Defines the password of the user defined in the Search user field. The value of this field can be left blank if the Search user does not have a defined password.</td>
</tr>
<tr>
<td>URL</td>
<td>Defines URL address and port of a directory server, the DN of an entry within that server, or the criteria for performing a search within that server. ldap(s): //&lt;server&gt;://&lt;port&gt;</td>
</tr>
<tr>
<td>Base DN</td>
<td>Defines the starting domain name for the user search in the directory tree structure.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>: sales.company.us.com,dc=sales, dc=company,dc=us,dc=com. This field must have a value if the <strong>Search User</strong> field is left blank. Otherwise the default value is the domain where the search user is located.</td>
</tr>
<tr>
<td>Username Attribute</td>
<td>Defines the name of the LDAP attribute that determines the username. The search users perform a lookup for any login user on this attribute.</td>
</tr>
<tr>
<td>DN Attribute</td>
<td>Defines the name of the LDAP attribute that determines the user DN. After the search users perform lookup for any login user based on the <strong>Username Attribute</strong>, it verifies authentication with the user DN (which appears in the user's DN attribute).</td>
</tr>
<tr>
<td>Timeout</td>
<td>Determines the number of milliseconds to wait before a timeout (Default: 30000)</td>
</tr>
</tbody>
</table>

The following table describes the PAM authentication parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service name</td>
<td>Defines the PAM service name (default passwd)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: In non-root mode, you can only authenticate the Control-M/Agent user. To authenticate other users, you must run as root.</td>
</tr>
</tbody>
</table>
Control-M MFT Enterprise B2B

Control-M MFT Enterprise B2B is an MFT add-on that enables you to securely transfer and receive files to and from external users outside of your organization. Internal users can transfer files externally with File Transfer jobs, while external users transfer files to and from your organization via a BMC-provided web application or third-party FTP client.

To use Control-M MFT Enterprise B2B, you need to define external users and virtual folders. Virtual folders are the locations where external users transfer and receive files. Each folder has an incoming sub-folder where files are sent by external users to your organization, and an outgoing sub-folder where files are sent by internal users to external users. Authorizations are applied at the folder level to determine which external users can access the folders. Folders can be configured to define a maximum retention period and can generate email notifications to associated users when new files are available.

The following diagram shows the Control-M MFT Enterprise B2B architecture.

Control-M MFT Enterprise B2B includes the following main components:

- **MFT Enterprise B2B Hub**: The Hub is the File Transfer Server that is installed with Control-M MFT and is used to manage external file transfers. After MFT Enterprise B2B is enabled, the File Transfer Server configuration is managed in the Hub settings. The Hub allows internal and external users to log in, whereas the File Transfer Server only allows internal users to log in.

- **MFT Enterprise B2B Gateway**: A proxy server that is installed in the DMZ and listens for incoming SFTP, FTPS, and HTTPS connections from external user accounts defined in the MFT B2B Hub. The MFT Enterprise B2B Gateway communicates with the Hub but does not store any transfer file data.
  
  **NOTE**: REST API is also supported on an HTTPS connection. If you want to use REST API to access the B2B Gateway, you can see the REST API available calls/documentation at the following URL:

- **MFT Enterprise B2B File Exchange**: A web application that enables external users to view the contents of their folders, and upload and download files.

Files are transferred between the Hub (File Transfer Server) within your organization, and external users via the Control-M MFT Enterprise B2B Gateway in the DMZ.
To get started with Control-M MFT Enterprise B2B, see Setting up the Control-M MFT Enterprise B2B environment (on page 18).

Setting up the Control-M MFT Enterprise B2B environment

This procedure describes how to set up the Control-M MFT Enterprise B2B environment.

Before you begin

Ensure that you have installed the following:

- Control-M/EM 9.0.18
- Control-M/Server 9.0.18
- Control-M/Agent 9.0.18 or higher

➢ To set up:

1. Install the Control-M MFT Deployment package on a Control-M/EM server 9.0.19, as described in Control-M Managed File Transfer installation (on page 7).


3. Deploy Control-M MFT 9.0.19 to at least one Control-M/Agent.


5. Install Control-M MFT B2B Gateway in the DMZ on a Linux computer, as described in Installing the Control-M MFT Enterprise B2B Gateway on Linux (on page 20).


7. Create External users (on page 22) and Virtual Folders (on page 23).

8. Provide external users with their login credentials (username, password, and port) to the MFT Enterprise B2B File Exchange website or third-party FTP client.

9. Create an SFTP connection profile using the Hub as the host with port 1222, as described in Creating a connection profile (on page 34).

10. Transfer files between external and internal users, as described in Defining a File Transfer job (on page 35).
Installing Control-M MFT Enterprise B2B on Windows

This procedure describes how to install Control-M MFT Enterprise B2B on a Control-M/EM server on Windows.

Before you begin

- Ensure that the database server that contains the Control-M/EM database is up and running.

To install MFT Enterprise B2B on Windows:


2. Do one of the following:
   - Interactive install: Follow the on-screen instructions until the installation is complete.
   - Automatic install: Create a parameter file and then run the automatic install in a non-interactive mode, as follows:
     a. Follow the on-screen instructions until the Summary window.
     b. Click Generate and select the location to create the XML parameter file.
     c. Click Yes to quit the installation. A confirmation message appears.
     d. Click Yes.
     e. Copy the automatic installation parameters file to a network location that is accessible to all computers where you want to perform an automatic installation.
     f. Log in using a user ID that has Administrator permissions on the current computer.
     g. Ensure that the installation DVD is still in the DVD drive, and run the installation script, as follows:
        
        `<source_path>\Setup.exe -silent <xml_path>|<filename.xml>`
        
        The installation log can be found at the following location:
        
        `<installFolder>\BMCI INSTALL\log\BMC_Control-M_MFT_B2B.Install_ <date-time>.log`

3. Click Done.
Installing Control-M MFT Enterprise B2B on UNIX

This procedure describes how to install Control-M MFT Enterprise B2B on a Control-M/EM server on UNIX.

Before you begin

- Ensure that the database server that contains the Control-M/EM database is up and running.

➢ To install MFT Enterprise B2B on UNIX:

1. Mount the installation CD from the root user and log off the root user before continuing with the installation.
2. Log in to the Control-M/EM account.
   
   **NOTE:** If you are using the GUI, set the environment variable `DISPLAY` to value `<hostName>:0.0`. It is not necessary to set `DISPLAY` for console mode or silent mode. (For more information, see Setting environment variables in UNIX.)
3. Type the following command:
   
   `<cdPath>/setup.sh`
4. Follow the on-screen instructions until the installation is complete.

Installing the Control-M MFT Enterprise B2B Gateway on Linux

This procedure describes how to install Control-M MFT Enterprise B2B Gateway on Linux in the DMZ. The Gateway is a proxy server used to transfer files to and from the Control-M MFT Enterprise B2B Hub by external users.

Before you begin


➢ To install MFT Enterprise B2B Gateway on Linux:

1. Mount the installation CD from the root user and log off the root user before continuing with the installation.

   **NOTE:** If you are using the GUI, set the environment variable `DISPLAY` to value `<hostName>:0.0`. It is not necessary to set `DISPLAY` for console mode or silent mode. (For more information, see Setting environment variables in UNIX.)
2. Type the following command:
   
   `<cdPath>/setup.sh`
3. Follow the on-screen instructions until the installation is complete.
4. Start up the MFT Enterprise B2B Gateway by running the following command:

   `mft-proxy/exe/start-mft-proxy.sh`

   **NOTE:** Verify that the Hub is up before restarting the Gateway.
Uninstalling Control-M MFT Enterprise B2B from Windows

This procedure describes how to uninstall Control-M MFT Enterprise B2B from Windows.

➢ To uninstall MFT Enterprise B2B from Windows:

1. From the Start menu, select Control Panel.
2. Double-click Programs and Features.
4. Click OK to continue.

Control-M MFT Enterprise B2B is successfully removed from your computer.

Uninstalling Control-M MFT Enterprise B2B from UNIX

This procedure describes how to uninstall Control-M MFT Enterprise B2B from UNIX.

➢ To uninstall MFT Enterprise B2B from UNIX:

1. Log in as a Control-M user.
2. Navigate to the following directory:
   
   \<InstallFolder>/BMCINSTALL/uninstall/DRM2B

3. Type one of the following commands:
   - Interactive uninstall: ./uninstall.sh
   - Automatic uninstall: ./uninstall.sh -silent

Control-M MFT Enterprise B2B is successfully removed from your computer.

Uninstalling Control-M MFT Enterprise B2B Gateway from Linux

This procedure describes how to uninstall Control-M MFT Enterprise B2B Gateway from Linux.

➢ To uninstall MFT Enterprise B2B Gateway from Linux:

1. Navigate to the following directory:
   
   \<InstallFolder>/BMCINSTALL/uninstall/DRM2B.9.0.19

2. Type one of the following commands:
   - Interactive uninstall: ./uninstall.sh
   - Automatic uninstall: ./uninstall.sh -silent

The Control-M MFT Enterprise B2B Gateway is successfully removed from your computer.

Enabling an MFT Enterprise B2B Hub

This procedure describes how to enable an MFT Enterprise B2B Hub, which allows file transfers to and from the Control-M MFT Enterprise B2B Gateway. The MFT Enterprise B2B Hub uses the File Transfer Server to transfer files.
After the Hub is enabled, all File Transfer Server configuration is managed from the Hub Settings (on page 24).

**NOTE:** You can enable one MFT Enterprise B2B Hub per Control-M/EM server.

➢ To enable an MFT Enterprise B2B Hub:

1. From the Manage tab, click **MFT B2B**.
   - If the button is disabled, you need to install Control-M MFT B2B, as described in Control-M MFT Enterprise B2B installation.
   - The **MFT B2B** window appears.

2. Click **Add Hub**.

3. Do the following:
   a. From the **Select B2B hub environment** drop-down list, select the host where Control-M MFT is installed.
      - **NOTE:** You can only select a Control-M MFT 9.0.18 or higher that is installed on a Control-M/Agent 9.0.18 or higher.
   b. In the **Gateway Authentication Password** field, type the same password you used when you installed the Control-M MFT Enterprise B2B Gateway.
   c. In the **Domain Name** field, type the domain name of the MFT Enterprise B2B File Exchange website where external users can transfer using HTTP.
      - **EXAMPLE:** or 172.99.98.77:<HTTP_Port>
   d. In the **Company Name** field, type the name of your company.
      - This name appears in the MFT Enterprise B2B File Exchange website and the email notification signature.
   e. In the **Company Support Email** field, type the email address that is used to send and receive email notifications to and from external users.

4. Click **Create**.
   - The MFT Enterprise B2B Hub is enabled.

**Creating external users**

This procedure describes how to create MFT Enterprise B2B external users, which enables them to transfer and receive files via the File Exchange website or a third-party FTP client.

**Before you begin**

➢ Enable an MFT Enterprise B2B Hub, as described in Enabling an MFT Enterprise B2B Hub (on page 21)

➢ To create external users:

1. From the Manage tab, click **MFT B2B**.
   - The **MFT B2B** window appears.

2. From the **Users** tab, click **+**.
3. Do the following:
   a. In the **User Name** field, type the name of the new external user.
   b. In the **Password** field, create a password for the external user.
   c. In the **Email** field, type the email address of this user.
   d. In the **Phone Number** field, type the phone number of the user.
   e. In the **Company Name** field, type the name of the organization that this user belongs to.
   f. In the **Description** field, provide a description of this user.
   g. In the **SSH Setting** area, in the **SSH Public Key** field, type the ssh-rsa key format.
   h. In the **AS2 Setting** area, do the following:
      a. In the **AS2 ID** field, type the logical name of the trading partner.
      b. In the **Partners Certificate Alias** field, type the alias of the partner certificate that is stored in the AS2 keystore.
      c. In the **AS2 Destination Folder**, select the authorized virtual folder where the uploaded file must be saved.
         If the virtual folder doesn't exist, the AS2 messages is stored in `/cm/AFT/as2/server/inbox`.

Creating Virtual Folders

This procedure describes how to create MFT Enterprise B2B Virtual Folders. These folders are used to transfer incoming and outgoing files between external and internal users. Authorizations are applied at the folder level that determine which external and internal users can access the folders. Folders can be configured to define a maximum retention period, and can generate email notifications to associated users when new files are available.

**Before you begin**

- Enable an MFT Enterprise B2B Hub, as described in [Enabling an MFT Enterprise B2B Hub](page 21).

**To create Virtual Folders:**

1. From the Manage tab, click **MFT B2B**.
   
   The **MFT B2B** window appears.

2. From the **Virtual Folders** tab, click .

3. Do the following:
   a. In the **Virtual Folder Name** field, type the name of the folder.

      By default, the following sub-folders are automatically created within this folder in the Hub environment:
      
      - **Incoming**: Files sent by external users to your organization.
      - **Outgoing**: Files sent by internal users to external users.
b. In the **Size Limit** field, type the maximum number of GB allowed before file uploading is blocked for external and internal users.

   **NOTE**: If the value is set to 0, files uploading is unlimited.

c. In the **Retention Time** field, type the maximum number of hours to keep the file, before it is automatically deleted.

   **NOTE**: If the value is set to 0, retention is unlimited.

   **NOTE**: If a file was uploaded with the SFTP -p option, which preserves file attributes, the file might be deleted. In this case, do not use the -p option or extend the retention, as required.

d. If you want to delete the file after an internal user has downloaded it from an incoming sub-folder, select the **Delete file after downloaded from incoming folder** option (*SFTP only*).

e. In the **Authorized External Users** field, type the names of the external users that you want to have access to this folder.

   To notify users that a file is ready for download from the Outgoing sub-folder, select the **Send email notification to allowed users when a new file arrives** checkbox.

f. In the **Allowed Internal Users** field, type the names of internal users that you want to have access to this folder.

   For all internal users, type *.

g. In the **Allowed File Pattern** field, type the file pattern that you want to allow external users to upload to this folder.

   **NOTE**: By default, all files are allowed to a folder.

   **EXAMPLE**: *.txt,Receipt*.pdf

h. In the **Blocked File Pattern** field, type the file pattern that you want to exclude external users from uploading to this folder.

4. Click **Save**.

   The folder is created.

**Hub Settings**

The Hub settings are pre-configured and are based on the settings you have defined in the File Transfer Server.

The following lists the Hub settings options:

- **General Settings** (on page 25)
- **Authentication Settings** (on page 26)
- **HTTP Settings** (on page 27)
- **SFTP Settings** (on page 28)
- **FTP/S Settings** (on page 29)
- **Authentication Settings** (on page 31)
- **Notification Settings** (on page 32)
General Settings

The following table describes the Hub general setting parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub Name</td>
<td>Defines the logical name of the Hub.</td>
</tr>
<tr>
<td>Home Directory</td>
<td>Defines the root path where transferred files are stored.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you want to use a different directory for each logged in internal user, you must add ${userName} to the path.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>: C:\temp,${userName}</td>
</tr>
<tr>
<td></td>
<td>Bob connects to the File Transfer Server and uploads the file a.txt to the root directory, the file is saved in</td>
</tr>
<tr>
<td></td>
<td>C:\temp\Bob\a.txt.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: &lt;Agent_Home&gt;/CM/AFT/ftshome/${userName}</td>
</tr>
<tr>
<td>B2B Subfolder</td>
<td>Defines the name of the folder under the home directory that contains all the Virtual Folders.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: For internal users, this folder is hidden. Internal user can only access the B2B virtual folders by typing the B2B sub-folder</td>
</tr>
<tr>
<td></td>
<td>under the home dir.</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>: /b2bhome/</td>
</tr>
<tr>
<td>Configuration Port</td>
<td>Determines the port number used to access the Hub for configuration changes.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 28080</td>
</tr>
<tr>
<td>Send Audit Logs</td>
<td>Determines whether to generate records to the database.</td>
</tr>
<tr>
<td>Log Level</td>
<td>Determines one of the following log levels for the Hub:</td>
</tr>
<tr>
<td></td>
<td>▪ ERROR</td>
</tr>
<tr>
<td></td>
<td>▪ WARN</td>
</tr>
<tr>
<td></td>
<td>▪ INFO</td>
</tr>
<tr>
<td></td>
<td>▪ DEBUG</td>
</tr>
<tr>
<td></td>
<td>▪ TRACE</td>
</tr>
</tbody>
</table>
### Authentication Settings

The following table describes the Hub authentication parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Authentication Password</td>
<td>Determines the authentication password between the MFT Enterprise B2B Gateway and the Hub. This is the same password set during the MFT Enterprise B2B Gateway installation.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you change the password, you must also define the new password in <code>proxyConfig.properties</code> file on the host where the Gateway is installed and restart the Gateway.</td>
</tr>
<tr>
<td>Internal users authentication method (SFTP/FTP)</td>
<td>Determines one of the following authentication methods for internal users for both SFTP and FTP:</td>
</tr>
<tr>
<td></td>
<td>- Windows Local Users (<em>Windows only</em>)</td>
</tr>
<tr>
<td></td>
<td>- PAM (<em>UNIX only</em>)</td>
</tr>
<tr>
<td></td>
<td>- LDAP</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> (PAM) You can only authenticate the Control-M/Agent user in non-root mode. To authenticate other users, you must run as root.</td>
</tr>
</tbody>
</table>
## HTTP Settings

The following table describes HTTP Settings for the MFT Enterprise B2B File Exchange web application.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>Determines the HTTP or HTTPS port number for the MFT Enterprise B2B File Exchange.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you change this parameter in Gateway Settings, you must change it in the proxyConfig.properties file in the Gateway and restart the Gateway.</td>
<td></td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Determines whether to enable HTTPS.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you change this parameter, you must change it in the Hub and Gateway settings and in the hub.ssl parameter in the proxyConfig.properties file in the Gateway and restart the Gateway.</td>
<td></td>
</tr>
<tr>
<td>Keystore File Path</td>
<td>Determines the path for the HTTPS keystore file.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The keystore must be in <strong>PKCS12</strong> format. If FIPS is enabled, the format must be <strong>BCFKS</strong>.</td>
<td></td>
</tr>
<tr>
<td>Keystore File Password</td>
<td>Determines the password that is used by the Hub to access the HTTPS keystore.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: password (Hub), abcd1234 (Gateway)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you change this password, the keystore password is not changed. For more information, see Changing the MFT key database password.</td>
<td></td>
</tr>
<tr>
<td>Session Timeout</td>
<td>Determines the number of seconds to wait before a timeout.</td>
<td>Hub Settings</td>
</tr>
</tbody>
</table>
## SFTP Settings

The following table describes the SFTP settings between the Hub and the MFT Enterprise B2B Gateway.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
</table>
| SFTP Port          | Determines the port number that the embedded Hub/Gateways listens to for SFTP connections.  
                      **NOTE:** This port is used by clients to connect to the SFTP server.  
                      **Default:** 1222 (Hub), 1224 (Gateway). | Hub Settings  
                                          Gateways Settings |
| Keystore File Path | Defines the path to the file that contains the client's certificate.  
                      **NOTE:** The keystore must be in PKCS12 format.  
                      If FIPS is enabled, the format must be BCFKS. | Hub Settings  
                                          Gateways Settings |
| Keystore File Password | Defines the password for the file that contains the server's certificate.  
                           **Default:** abcd1234  
                           **NOTE:** If you change this password, the keystore password is not changed. For more information, see Changing the MFT key database password. | Hub Settings  
                                          Gateways Settings |
| Allowed Ciphers    | Determines the cipher security settings used for SFTP. | Hub Settings  
                                          Gateways Settings |
| Authorized Keys File Path | Defines the path to the file that contains authorized users by SFTP.  
                           **NOTE:** The authorized users file must include all internal users' public keys. Each user should be included in the following format:  
                           `<username> <ssh public key (ssh-rsa format)>` | Hub Settings |
FTP/S Settings

The following table describes FTP/S settings between the Hub and the MFT B2B Gateway.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen for FTP/S connection</td>
<td>Determine whether the Hub/Gateway that supports client connection with the FTP/FTPS protocol is enabled.</td>
<td>Hub Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When internal users connect with FTP/S, they cannot access the B2B sub-folder. To access the B2B sub-folder from inside the organization, use SFTP protocol.</td>
<td></td>
</tr>
<tr>
<td>FTP Port</td>
<td>Determines the port number that the embedded Hub/Gateway listens to for FTP/FTPS connections.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This port is used by clients to connect to the FTP/FTPS server</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1221 (Hub), 1223 (Gateway).</td>
<td></td>
</tr>
<tr>
<td>Allow multiple open sessions</td>
<td>Determines whether multiple users can connect to the Hub/Gateway simultaneously.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Maximum Concurrent Open Sessions</td>
<td>Determines the number of users that can connect to the Hub/Gateway simultaneously.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Maximum Login Failures</td>
<td>Determines the maximum number of login attempts before a timeout.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Delay Between Login Failures</td>
<td>Determines the number of seconds to wait after a login failure before the next attempt.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Secured FTP Enabled</td>
<td>Determines whether FTPS is enabled.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If you change this parameter, you must change it in the Hub and Gateway settings and in the <strong>hub.ssi</strong> parameter in the <strong>proxyConfig.properties</strong> file in the Gateway and restart the Gateway</td>
<td></td>
</tr>
<tr>
<td>Keystore File Path</td>
<td>Defines the path to the file that contains the server certificate.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The keystore must be in <strong>PKCS12</strong> format. If FIPS is enabled, the format must be <strong>BCFKS</strong>.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Location</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Keystore File Password</td>
<td>Defines the password of the file that contains the server certificate.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: password (Hub), abcd1234 (Gateway)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If you change this password, the keystore password is not changed. For more information, see Changing the MFT key database password.</td>
<td></td>
</tr>
<tr>
<td>Allowed Ciphers</td>
<td>Determines the cipher security settings used for FTPS.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Listen for Implicit Connection</td>
<td>Determines whether to automatically turn on security after a connection is established between the FTPS client and the Managed File Transfer server.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td>Passive Ports</td>
<td>Limits the range of dynamic ports that can be used for passive connections in FTP. Ports can be defined as single ports, closed or open ranges. Multiple definitions must be separated by commas.</td>
<td>Hub Settings, Gateways Settings</td>
</tr>
<tr>
<td></td>
<td><strong>EXAMPLE</strong>:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2300 : Uses 2300 as the passive port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2300-2399: Uses all ports in the range</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2300-: Uses all ports larger than 2300</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2300,2305,2400-: Uses 2300 or 2305 or any port larger than 2400</td>
<td></td>
</tr>
</tbody>
</table>
## Authentication Settings

The following table describes the LDAP or PAM settings for the Hub. These parameters are for internal users only.

<table>
<thead>
<tr>
<th>Table Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Search User</td>
<td>Defines the LDAP Browse user.</td>
</tr>
<tr>
<td>LDAP Search Password</td>
<td>Defines the password of the user defined in the LDAP Search User field. The value of this field can be left blank if the Search user does not have a defined password.</td>
</tr>
<tr>
<td>LDAP Server URL</td>
<td>Defines URL address and port of a directory server, the DN of an entry within that server, or the criteria for performing a search within that server. ldap(s)://&lt;server&gt;:&lt;port&gt;</td>
</tr>
</tbody>
</table>
| Base DN            | Defines the starting domain name for the user search in the directory tree structure.  
  **EXAMPLE**: sales.company.us.com,dc=sales,  
  dc=company,dc=us,dc=com.     
  This field must have a value if the **LDAP Search User** field is left blank. Otherwise the default value is the domain where the search user is located. |
| Home Directory     | Defines the LDAP Home Directory.                                            |
| Timeout            | Determines the number of milliseconds to wait before a timeout.             |

The following table describes the PAM authentication parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Service name| Defines the PAM service name (default passwd)  
  **NOTE**: In non-root mode, you can only authenticate the Control-M/Agent user. To authenticate other users, you must run as root. |
Notification Settings

The following table describes notification settings that enables MFT Enterprise B2B to send email notifications to external users that files have arrived.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Host</td>
<td>Defines the hostname that sends the email notifications.</td>
</tr>
<tr>
<td>SMTP Port</td>
<td>Defines the SMTP port number.</td>
</tr>
<tr>
<td>SMTP Username</td>
<td>Defines the username that is used to send the notifications.</td>
</tr>
<tr>
<td>SMTP Password</td>
<td>Defines the SMTP password.</td>
</tr>
<tr>
<td>SMTP Security Method</td>
<td>Determines one of the following SMTP security methods:</td>
</tr>
<tr>
<td></td>
<td>▪ SMTP without TLS</td>
</tr>
<tr>
<td></td>
<td>▪ SMTP with STARTTLS</td>
</tr>
<tr>
<td></td>
<td>▪ SMTPS (SMTP over TLS)</td>
</tr>
<tr>
<td>Sender Address</td>
<td>Defines the email address that is used to send the email notification.</td>
</tr>
<tr>
<td>Sender Name</td>
<td>Defines the name of the sender that appears on the notification mail signature.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If this field is left empty, then the Company Name defined in Site Settings (on page 33) is used.</td>
</tr>
</tbody>
</table>
Gateway Settings

The following table describes the MFT Enterprise B2B Gateway settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Defines the MFT Enterprise B2B File Exchange website domain name that is accessed by external users. http(s)://&lt;domain_name&gt;:&lt;HTTP_port&gt;</td>
</tr>
<tr>
<td>Log Level</td>
<td>Determines one of the following log levels for the Gateway:</td>
</tr>
<tr>
<td></td>
<td>● ERROR</td>
</tr>
<tr>
<td></td>
<td>● WARN</td>
</tr>
<tr>
<td></td>
<td>● INFO</td>
</tr>
<tr>
<td></td>
<td>● DEBUG</td>
</tr>
<tr>
<td></td>
<td>● TRACE</td>
</tr>
<tr>
<td>HTTP Settings</td>
<td>See HTTP Settings (on page 27).</td>
</tr>
<tr>
<td>SFTP Settings</td>
<td>See SFTP Settings (on page 28).</td>
</tr>
<tr>
<td>FTP/S Settings</td>
<td>See FTP/S Settings (on page 29).</td>
</tr>
<tr>
<td>AS2 Settings</td>
<td>See AS2 Settings</td>
</tr>
</tbody>
</table>

Site Settings

The following table describes the File Exchange settings for each external web application.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Defines your company name that appears in the MFT Enterprise B2B File Exchange web application and email notification signature.</td>
</tr>
</tbody>
</table>
| Company Support Email| Defines your company's email address that is available for external users from the File Exchange web application and as the sender address for email notifications.  
  **NOTE:** This field can be overwritten by the **Sender Name** field in Notification Settings (on page 32). |
Creating a connection profile

This procedure describes how to create an MFT connection profile in the Control-M Configuration Manager, which enables you to define a File Transfer job in the Control-M.

**NOTE:** If you are defining a connection profile for MFT Enterprise B2B on the File Transfer Server (Hub), you must define it as SFTP.

**Before you begin**

If you want to use key authentication to access an SFTP server, you need to generate an SSH key, as described in Generating SSH keys.

**To create a connection profile:**

1. From Control-M Configuration Manager, select the **Control-M for IBM Cognos** on the host that you want to manage and right-click **Connection Profile Management**.

   The **Managed File Transfer - Connection Profile Management** dialog box appears.

2. Click the **icon.**

   The **Add Connection Profile** dialog box appears.

3. In the **Connection Profile Name** field, type the name of the connection profile that you want to add (The connection profile name must begin with a letter and without any blanks or special characters).

4. In the **Connection Profile Type** area, select one of the following:
   - **File transfer single endpoint:** Transfers files from the host defined in this connection profile to hosts defined in multiple connection profiles. Select this option if you want to reuse this connection profile to transfer files to different hosts.
   - **File transfer dual endpoint:** Transfers files between two specific hosts defined in this connection profile.
   - **File transfer group:** See Creating a file transfer group connection profile.

5. In the **Control-M Users** table, do one of the following:
   a. To select users from the list, select the users that you want to allow access to this connection profile, click **Add**, and then click **Next**.
   b. To add users or groups manually, , click **Add Manually.**

   The **Authorized User or Group** dialog box appears.
   a. In the **Add EM user or group** field, type the name of the user or group you want to add.

   Multiple users and groups must be separated by a | character.

   b. In the **Type** area, select **User** or **Group**.

   c. Click **OK**.

   **NOTE:** Wildcard characters (* and?) can be used as part of a defined Control-M/EM user or group.

   The **Set Host1 details** dialog box appears.

6. For each field, type the required value, as described in Control-M for MFT connection profile parameters.
7. If you have defined this host as a Local CM, continue to step 8, otherwise, in the Communication Protocol area, select one of the following options, and then click **Next**:
   
   a. **FTP**: File Transfer Protocol. For each field, type the required value, as described in FTP protocol parameters.

   b. **SFTP (SSH)**: Secure File Transfer Protocol. For each field, type the required value, as described in SFTP (SSH) protocol parameters.

   c. **S3**: Amazon Simple Storage Service. For each field, type the required value, as described in S3 protocol parameters.

   d. **AS2**: Applicability Statement. For each field, type the required value, as described in AS2 parameters.

   The **Set Host2 details** dialog box appears. If you are defining one host, continue with step 10.

8. For each field, type the required value as described in Control-M for MFT connection profile parameters.

9. Repeat steps to set Host2, and then click **Next**.

   The **Set Additional Settings** dialog box appears.

10. For each field, type the required value as described in Connection profile additional parameters, and then click **Next**.

   If you want to manually add additional parameters for a single connection profile, in the Manual Additional Parameters area, add new parameters, as described in Connection profile manual parameters.

   The **Add Connection Profile - Summary** dialog box appears.

11. Review the connection profile details and click **Test** *(optional)* or **Finish**.

   If the test completed successfully, the connection profile is validated and you can now define a MFT job, as described in Defining a Control-M for PeopleSoft job. If the test failed, review the error message and test it again.

   **NOTE**: In AS2, a test file is sent to the AS2 server.

   The connection profile is added to the **Control-M for MFT - Connection Profile Management** dialog box.

---

### Defining a File Transfer job

This procedure describes how to define a File Transfer job, which enables you to watch and transfer files from a local host to a remote host, a remote to a local host, or a remote host to another remote host.

**NOTE**: Control-M for AFT jobs on Control-M/Agent and Control-M MFT jobs on another Control-M/Agent cannot belong to the same Host group.

**Before You Begin**

Ensure that you have met the following requirements:
To define a File Transfer job:

1. In the **General** tab, from the **Connection Profile** field, click .
   The **Select Connection Profile** dialog box appears.
2. In the Connection Profile Type area, select one of the following:
   - **Endpoint1 <-> Endpoint2**: Shows connection profiles that are defined with two hosts. Select this option if the source and destination locations are defined in the same connection profile.
   - **Two Single Endpoints**: Shows connection profiles that are defined with one host. Select this option if the source and destination locations are defined in separate connection profiles.
   
   **NOTE:**
   - If you are transferring a file to an external user, you must select the connection profile that is connected to the Hub that uses an SFTP protocol.
   - AS2 and S3 connection profiles can be paired with Local connection profiles only. FTP and SFTP are not supported.
3. Select the connection profile(s) that you want to use to transfer files, and click **OK**.
4. If you are transferring a file to or from S3, in the **Bucket** field, click and select an Amazon S3 bucket.
5. In the **Transfers** area, do the following:
   a. In the **Transfers** area, in the first field browse for the file, directory, or library to transfer. You can also type the path manually.
      
      **NOTE:** If you are transferring a file to an external user, you must type in the B2B Subfolder home directory (example: /b2bhome) that is defined in MFT Enterprise B2B settings, as described in **General Settings** (on page 25).
      
      **NOTE:** In AS2, you cannot determine the destination file path. You can override the destination filename, subject, and content type.
   
   b. In the second field, browse for the file, directory, or library to transfer. You can also type the path manually. If you are transferring a file to multiple hosts, select one of the following:
      
      o **Home Directory**: Transfer the file to the home directory on each host.
      
      o **Common Destination Path**: Transfers the file to the same location on each host defined here.
      
      o **Different Destination Paths**: Transfers the file to different destinations on each host. Click and define each path by browsing to each file in **File Selection** or modify the locations in one view in **Paths List**.
   
   c. Select the transfer option, as described in Transfer options.
NOTE: You can transfer up to five files at a time, but file transfers within a job are sequential, which means that if a file transfer fails, subsequent file transfer definitions are not performed, unless you select the **Continue on failure** checkbox, as described in Advanced general parameters.

NOTE: If a transfer has CJK or Latin-1 characters in the filename, the Control-M/EM server and Control-M/Server databases must be compatible with this format.

6. From the **Type** drop-down list, select the transfer format. EBCDIC format is supported only when transferring files between two MVS FTP hosts.

7. Click **Advanced**.

   The **Advanced** dialog box appears.

8. Select the required options, as described in Advanced options, and click **OK**.

9. Select the optional parameters if required, as described in Optional parameters.

10. Click **More**.

    The **Pre-execution Command** and **Post-execution Command** fields are used to define specific commands to execute at the beginning or at the end of a job. These commands can only be executed on a computer where Control-M/Agent is installed, and the output of the commands (pre or post) appears in the job output.