



Control-M Managed File Transfer 9.0.00.500 Setup Guide



June 2017



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** **Telephone** ■ **713 918 8800** **Fax** **713 918 8000**
 2103 CITYWEST BLVD ■ **800 841 2031**
 HOUSTON TX
 77042-2827
 USA

Outside United States and Canada

Telephone **(01) 713 918 8800** **Fax** **(01) 713 918 8000**

© Copyright 1999-2017 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”) or Microsoft Azure (“Azure”) cloud environment, a license is required for the total number of CPUs in each AWS or Azure instance upon which the Product is installed or which the Product manages, either remotely or locally. For AWS, 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 platforms onto which one or more application plug-ins are installed but also includes Control-M Agent platforms where no application plug-ins are installed.

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 iSeries, 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	10
Configuring the File Transfer Server	11

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 9.0.00.300 or higher, as described in [Control-M/EM 9.0.00.300 Release Notes](#).
- Install Control-M/Server 9.0.00.200 or higher, as described in [Control-M/Server 9.0.00.200 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).

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 9.0.00** wizard appears.
2. Do one of the following:
 - **Interactive install:** Follow the on-screen instructions until the installation is complete.
 - **Automatic install:** Do the following:
 - 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 <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 9.0.00**, 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.9.0.00
```
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 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:

- **Transfer Package:** 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.
- **Transfer and Automatically Install Package:** Transfers the MFT installation package to specific Control-M/Agent computers and begins the upgrade process automatically.

NOTE:

- 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 Control-M/Agent 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 12)
- [FTP/FTPS server parameters](#) (on page 13)
- [SFTP server parameters](#) (on page 14)
- [File Transfer Server Authentication parameters](#) (on page 15)

3. Click **Save**.

The File Transfer Server restarts and the changes are activated.

File Transfer Server general parameters

The following table describes File Transfer Server general parameters.

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

FTP/FTPS server parameters

The following table describes FTP/FTPS server parameters.

Parameter	Description
Enable server	Determine whether the File Transfer Server that supports client connection with the FTP/FTPS protocol is enabled
Port	Determines the port number that the embedded File Transfer Server listens to for FTP/FTPS connections NOTE: This port is used by clients to connect to the FTP/FTPS server (Default: 1221).
Authentication	Authenticates the FTP user with one of the following methods: <ul style="list-style-type: none"> ▪ Windows local user ▪ LDAP ▪ PAM (<i>UNIX only</i>)
Secured	Determines whether FTPS is enabled
Keystore file path	Defines the path to the file that contains the server certificate
Keystore file password	Defines the password of the file that contains the server certificate
Ciphers	Determines the cipher security settings used for FTPS
Listen for implicit connections	Determines whether to automatically turn on security after a connection is established between the FTPS client and the Managed File Transfer server.
Passive Port/s:	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. EXAMPLE: 2300 :Uses 2300 as the passive port 2300-2399 :Uses all ports in the range 2300- :Uses all ports larger than 2300 2300, 2305, 2400- : Uses 2300 or 2305 or any port larger than 2400

SFTP server parameters

The following table describes SFTP server parameters.

Parameter	Description
Enable server	Determines whether the File Transfer Server that supports client connection with SFTP is enabled
Port	Determines the port number that the embedded File Transfer Server listens to for SFTP connections NOTE: This port is used by clients to connect to the SFTP server (Default: 1222).
Keystore file path	Defines the path to the file that contains the client's certificate
Keystore file password	Defines the password for the file that contains the server's certificate
Ciphers	Determines the cipher security settings used for SFTP
Known user file path	Defines the path to the file that contains known users by SFTP
Authentication	Authenticates the FTP user with one of the following methods: <ul style="list-style-type: none"> ▪ Windows local user ▪ LDAP ▪ PAM (<i>UNIX only</i>)

File Transfer Server Authentication parameters

The following table describes File Transfer Server Authentication parameters.

Parameter	Description
PAM (UNIX only)	Authenticates the FTP user with PAM
Service name	Defines the PAM service name (default password)
LDAP	Authenticates the FTP user with LDAP
Admin user	Defines the LDAP Browse user
Admin password	Defines the LDAP Browse password
URL	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
Base DN	Determines the point from where a server searches for users
Home Directory	Defines the LDAP Home Directory
Timeout	Determines the number of minutes to wait before a timeout



491381