Configure Managed File Transfer

Managed File Transfer Overview

Managed File Transfer (MFT) allows an IM and Presence Service client, such as Cisco Jabber, to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

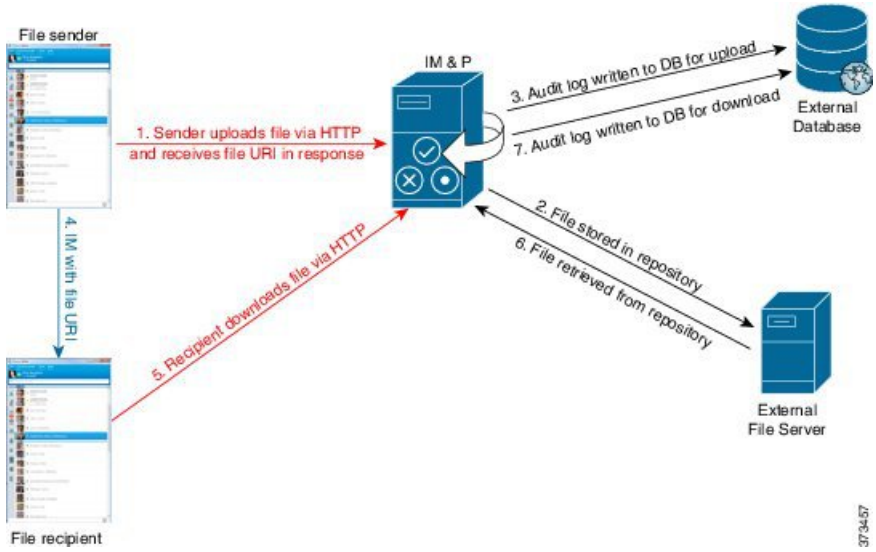
To deploy the Managed File Transfer feature, you must also deploy the following servers:

- **External database**—All file transfers get logged to the external database.
- **External File Server**—A copy of each transferred file gets saved to the repository on the external file server.

Note This configuration is specific to file transfers and has no impact on the message archiver feature for regulatory compliance.

For use cases, see Managed File Transfer Call Flow, on page 2

Managed File Transfer Call Flow



1. The sender uploads the file to the IM and Presence Service server via HTTP, and the server responds with a URI for the file.
2. The IM and Presence Service server sends the file to the file server repository for storage.
3. IM and Presence Service writes an entry to the external database log table to record the upload.
4. The sender sends an IM to the recipient. The IM includes the URI of the file.
5. The recipient sends an HTTP request to IM and Presence Service for the file. IM and Presence Service reads the file from the repository (6), records the download in the log table (7) and sends the file to the recipient.

The flow for transferring a file to a group chat or persistent chat room is similar, except the sender sends the IM to the chat room, and each chat room participant sends a separate request to download the file.

Note When a file upload occurs, the managed file transfer service is selected from all managed file transfer services available in the enterprise for the given domain. The file upload is logged to the external database and external file server associated with the node where this managed file transfer service is running. When a user downloads this file, the same managed file transfer service handles the request and logs it to the same external database and the same external file server, regardless of where this second user is homed.

Managed File Transfer Prerequisites

- You must also deploy an external database and external file server.
- Ensure that all clients can resolve the full FQDN of the IM and Presence Service node to which they are assigned. This is needed in order for Managed File Transfer to work.

External Database Prerequisites

Tip If you are also deploying persistent chat and/or message archiver, you can assign the same external database and file server for all features. Make sure when determining server capacity to consider the potential IM traffic, number of files transferred, and the file size.

Install and configure an external database. For details, including supported databases, see *Database Setup Guide for the IM and Presence Service*.

In addition follow these guidelines:

- You require one unique logical external database instance for each IM and Presence Service node in an IM and Presence Service cluster.
- The external database is supported on both virtualized and non-virtualized platforms.
- For a full list of the logged metadata, see the AFT_LOG Table in the "External Database Tools" chapter of the *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.
- If you are connecting to the external database using IPv6, check Configure IPv6 Task Flow for details on setting up IPv6.

External File Server Requirements

Follow these guidelines when setting up your external file server:

- Subject to file server capacity, each IM and Presence Service node requires its own unique Cisco XCP File Transfer Manager file server directory, however, nodes can share the same physical file server installation.
- The file server must support an ext4 file system, SSHv2, and SSH tools.
- The file server must support OpenSSH version between 4.9, 6.x, and 7.x.

Important This note is applicable for release 14SU3 onwards.

Note OpenSSH version 8.x is supported from release 14SU3 onwards.

- The network throughput between IM and Presence Service and the external file server must be greater than 60 megabytes per second.

  You can use the `show fileserver transferspeed` CLI command after you enable managed file transfer to determine your file server transfer speed. Be aware that if you run this command while the system is busy, it may impact the value returned by the command. For more information about this command, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* at this link.

Partition Recommendations for External File Servers

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

- If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
- Consider the number of uploads per day and the average file size.
- Ensure that the partition has sufficient disk space to hold the expected volume of files.
- For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

Directory Structure for External File Servers

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

User Authentication for the External File Server

IM and Presence Service authenticates itself and the file server using SSH keys:

- IM and Presence Service public key is stored on the file server.
- During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note The node public key is invalidated if the node's assignment is removed. If the node is reassigned, a new node public key is automatically generated and the key must be reconfigured on the external file server.

External File Server Requirements

Follow these guidelines when setting up your external file server:

- Subject to file server capacity, each IM and Presence Service node requires its own unique Cisco XCP File Transfer Manager file server directory, however, nodes can share the same physical file server installation.
- The file server must support an ext4 file system, SSHv2, and SSH tools.
- The file server must support OpenSSH version between 4.9, 6.x, and 7.x.

Important This note is applicable for release 14SU3 onwards.

Note OpenSSH version 8.x is supported from release 14SU3 onwards.

- The network throughput between IM and Presence Service and the external file server must be greater than 60 megabytes per second.

  You can use the `show fileserver transferspeed` CLI command after you enable managed file transfer to determine your file server transfer speed. Be aware that if you run this command while the system is busy, it may impact the value returned by the command. For more information about this command, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* at this link.

Partition Recommendations for External File Servers

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

- If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
- Consider the number of uploads per day and the average file size.
- Ensure that the partition has sufficient disk space to hold the expected volume of files.
- For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

Directory Structure for External File Servers

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

User Authentication for the External File Server

IM and Presence Service authenticates itself and the file server using SSH keys:

- IM and Presence Service public key is stored on the file server.
- During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note The node public key is invalidated if the node's assignment is removed. If the node is reassigned, a new node public key is automatically generated and the key must be reconfigured on the external file server.

Partitions Recommendations for External File Server

Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

Consider the following:

- If you create partitions, be sure to consider that the IM and Presence Service default file size setting (0) allows files up to 4GB to be transferred. This setting can be lowered when you set up managed file transfer.
- Consider the number of uploads per day and the average file size.
- Ensure that the partition has sufficient disk space to hold the expected volume of files.
- For example, 12000 users transfer 2 files per hour with an average file size of 100KB = 19.2GB per 8 hour day.

External File Server User Authentication

IM and Presence Service authenticates itself and the file server using SSH keys:

- IM and Presence Service public key is stored on the file server.
- During connection, SSHFS validates the IM and Presence Service private key. This ensures that the content of all files is encrypted.
- The file server public key is stored on IM and Presence Service. This allows the IM and Presence Service to ensure that it is connecting to the configured file server and minimizes man-in-the-middle attacks.

Note The node public key is invalidated if the node's assignment is removed. If the node is reassigned, a new node public key is automatically generated and the key must be reconfigured on the external file server.

External File Server Directory Structure

When the first file transfer occurs, timestamped subdirectories are automatically created, as described in this example:

- We create the path `/opt/mftFileStore/node_1/` on an IM and Presence Service node.
- The directory `/files/` is autogenerated.
- The three `/chat_type/` directories (`im`, `persistent`, `groupchat`) are autogenerated.
- The date directory `/YYYYMMDD/` is autogenerated.
- The hour directory `/HH/` is autogenerated. If more than 1,000 files are transferred within an hour, additional roll-over directories `/HH.n/` are created.
- The file is saved with an autogenerated encoded resource name, hereafter referred to as `file_name`.

In this example, our complete path to a file is:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

Using our example path:

- Files transferred during one-to-one IM on August 11th 2014 between 15.00 and 15.59 UTC are in the following directory: `/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  Files transferred during persistent group chat on August 11th 2014 between 16.00 and 16.59 UTC are in the following directory:
  `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- The 1001st file transferred during ad hoc chat on August 11th 2014 between 16.00 and 16.59 UTC is in the following directory:
  `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- If no file transfers occur inside of an hour, there are no directories created for that period.

Note The traffic between IM and Presence Service and the file server is encrypted using SSHFS, but the file contents are written to the file server in unencrypted form.

Managed File Transfer Task Flow

Complete these tasks to set up the Managed File Transfer feature on IM and Presence Service, and to set up your external file server.

Before you begin

Set up both an external database and an external file server for Managed File Transfer. For requirements, see

- External Database Prerequisites, on page 3
- External File Server Requirements, on page 3

For details on how to configure an external database, see the *External Database Setup Guide for the IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Procedure

	Command or Action	Purpose
Step 1	Add External Database Connection, on page 9	Configure a connection to the external database from the IM and Presence Service.
Step 2	Set up an External File Server, on page 10	Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.
Step 3	Create User for the External File Server, on page 11	Set up a user for the external file server.
Step 4	Set up Directory for External File Server, on page 12	Set up the top level directory structure for the external file server.
Step 5	Obtain Public Key for the External File Server, on page 13	Obtain the external file server's public key.
Step 6	Provision External File Server on IM and Presence Service, on page 14	Obtain the following information for the external file server:
Step 7	Verify Cisco XCP File Transfer Manager Activation, on page 16	The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.
Step 8	Enable Managed File Transfer, on page 17	Enable Managed File Transfer on IM and Presence Service.
Step 9	Verify External Server Status, on page 18	Verify that there are no problems with the external database setup and with the external file server setup.

Add External Database Connection

Configure a connection to the external database from the IM and Presence Service. With Managed File Transfer, you require a unique logical external database instance for each IM and Presence Service cluster node.

Before you begin

Set up each external database. For details, see the *External Database Setup Guide for the IM and Presence Service* at:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Messaging** > **External Servers Setup** > **External Databases**.

Step 2 Click **Add New**.

Step 3 In the **Database Name** field, enter the name of external database instance.

Step 4 From the **Database Type** drop-down, select the type of external database that you are deploying.

Step 5 Enter the **User Name** and **Password information** for the database.

Step 6 In the **Hostname** field, enter the hostname or IP address of the database.

Step 7 Complete the remaining settings in the **External Database Settings** window. For help with the fields and their settings, refer to the online help.

Step 8 Click **Save**.

Step 9 Repeat this procedure to create connections to each external database instance.

Set up an External File Server

Before setting up users, directories, ownership, permissions and other tasks on the file server, set up the external file server.

Before you begin

Review the design recommendations for the external file server. For details, see External File Server Requirements, on page 3.

Procedure

Step 1 Install a supported version of Linux.

Step 2 Verify the file server supports SSHv2 and OpenSSH 4.9 or later by entering one of the following commands as root:

```
# telnet localhost 22

Trying ::1...

Connected to localhost.

Escape character is '^]'.

SSH-2.0-OpenSSH_5.3
```

Or

```
# ssh -v localhost

OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010

debug1: Reading configuration data /root/.ssh/config ...

...debug1: Local version string SSH-2.0-OpenSSH_5.3

...
```

Step 3 To allow private/public key authentication, make sure that you have the following fields in the `/etc/ssh/sshd_config` file, set to *yes*.

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

If these are commented out in the file, the setting can be left alone.

Tip To enhance security, you can also disable password log in for the file transfer user (*mftuser* in our example). This forces logging in only by SSH public/private key authentication.

Step 4 Cisco recommends that you create one or more separate partitions that are dedicated to file transfer storage so that other applications that run on the server do not write to it. All file storage directories should be created on these partitions.

What to do next

Create User for the External File Server, on page 11

Create User for the External File Server

Set up a user for the external file server.

Before you begin

Set up an External File Server, on page 10

Procedure

Step 1 On the file server as root, create a user for the managed file transfer feature. This user owns the file storage directory structure (our example uses *mftuser*) and force creation of the home directory (**-m**).

```
# useradd -m mftuser

# passwd mftuser
```

Step 2 Switch to the managed file transfer user.

```
# su mftuser
```

Step 3 Create a `.ssh` directory under the *~mftuser* home directory that is used as a key store.

```
$ mkdir ~mftuser/.ssh/
```

Step 4 Create an `authorized_keys` file under the `.ssh` directory that is used to hold the public key text for each managed file transfer enabled node.

```
$ touch ~mftuser/.ssh/authorized_keys
```

Step 5 Set the correct permissions for passwordless SSH to function.

```
$ chmod 700 ~mftuser (directory)
$ chmod 700 ~/.ssh (directory)
$ chmod 700 ~/.ssh/authorized_keys (file)
```

Note On some Linux systems these permissions may vary, depending on your SSH configuration.

What to do next

Set up Directory for External File Server, on page 12

Set up Directory for External File Server

Set up the top level directory structure for the external file server.

You can create any directory structure that you want, with any directory names. Be certain to create a directory for each managed file transfer-enabled node. Later, when you enable Managed File Transfer on IM and Presence Service, you must assign each directory to a node.

Important You must create a directory for each node that has managed file transfer enabled.

Note A file server partition/directory is mounted in the IM and Presence Service directory that is used to store files.

Before you begin

Create User for the External File Server, on page 11

Procedure

Step 1 Switch back to the root user.

```
$ exit
```

Step 2 Create a top-level directory structure (our example uses `/opt/mftFileStore/`) to hold directories for all of the IM and Presence Service nodes that have Managed File Transfer enabled.

```
# mkdir -p /opt/mftFileStore/
```

Step 3 Give *mftuser* sole ownership of the `/opt/mftFileStore/` directory.

```
# chown mftuser:mftuser /opt/mftFileStore/
```

Step 4 Give the *mftuser* sole permissions to the `mftFileStore` directory.

```
# chmod 700 /opt/mftFileStore/
```

Step 5 Switch to the *mftuser*.

```
# su mftuser
```

Step 6 Create a subdirectory under `/opt/mftFileStore/` for each managed file transfer enabled node. (Later, when you enable managed file transfer, you assign each directory to a node.)

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

Note

- These directories and paths will be used in the **External File Server Diectory** field that you configure when you provision the file server in Cisco Unified CM IM and Presence Administration.
- If you have multiple IM and Presence Service nodes writing to this file server, you must define a target directory for each node, as we did in our example for three nodes`{node_1,node_2,node_3}`.
- Within each node's directory, the transfer type subdirectories (`im`, `groupchat`, and `persistent`) are automatically created by IM and Presence Service, as are all subsequent directories.

What to do next

Obtain Public Key for the External File Server, on page 13

Obtain Public Key for the External File Server

Obtain the external file server's public key.

Before you begin

Set up Directory for External File Server, on page 12

Procedure

Step 1 To retrieve the file server's public key, enter:

```
$ ssh-keyscan -t rsa host
```

Where *host* is the hostname, FQDN, or IP address of the file server.

Warning

- To avoid a man-in-the-middle attack, where the file server public key is spoofed, you must verify that the public key value that is returned by the **ssh-keyscan -t rsa** *host* command is the real public key of the file server.
- On the file server go to the location of the `ssh_host_rsa_key.pub` file (in our system it is under `/etc/ssh/`) and confirm the contents of the public key file, minus the host (the host is absent in the `ssh_host_rsa_key.pub` file on the file server), matches the public key value returned by the command **ssh-keyscan -t rsa** *host*.

Step 2 Copy the result of the **ssh-keyscan -t rsa** *host* command, not what is in the `ssh_host_rsa_key.pub` file. Be certain to copy the entire key value, from the server hostname, FQDN, or IP address to the end.

Note In most cases the server key begins with the hostname or FQDN, although it may begin with an IP address.

For example, copy:

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==

(ellipses added).

Step 3 Save the result of the **ssh-keyscan -t rsa** *host* command to a text file. It is needed when you configure the file server during the *Deploy an External File Server on IM and Presence Service* procedure.

Step 4 Open the `authorized_keys` file you created and leave it open. You will need it later, when you provision the file server on the IM and Presence Service.

Note If you are unable to retrieve the public key, see Troubleshooting External File Server Public and Private Keys, on page 19 for further help.

What to do next

Provision External File Server on IM and Presence Service, on page 14

Provision External File Server on IM and Presence Service

You must configure one external file server instance for each node in your cluster that will have Managed File Transfer enabled.

The external file server instances do not need to be physical instances of the external file server. However, be aware that for a given hostname, you must specify a unique external file server directory path for each external file server instance. You can configure all the external file server instances from the same node.

Before you begin

Obtain Public Key for the External File Server, on page 13

Obtain the following information for the external file server:

- Hostname, FQDN, or IP address
- Public key

- Path to the file storage directory
- User name

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External File Servers**.

Step 2 Click **Add New**.
The **External File Servers** window appears.

Step 3 Enter the server details. For help with the fields and their configuration options, see External File Servers Fields, on page 15.

Step 4 Click **Save**.

Step 5 Repeat this procedure until you have created a separate external file server instance for each cluster node where managed file transfer is enabled.

What to do next

Verify Cisco XCP File Transfer Manager Activation, on page 16

External File Servers Fields

Field	Description
Name	Enter the name of the file server. Ideally the server name should be descriptive enough to be instantly recognized. Maximum characters: 128. Allowed values are alphanumeric, dash, and underscore.
Host/IP Address	Enter the hostname or IP address of the file server. **Note** • The value entered for the Host/IP Address field must match the beginning of the key that is entered for the External File Server Public Key field (follows). • If you change this setting, you must restart the Cisco XCP Router service.

Field	Description
External File Server Public Key	Paste the file server's public key (the key you were instructed to save to a text file) in to this field. If you did not save the key it can be retrieved from the file server by running the command: `$ ssh-keyscan -t rsa host` on the file server. Where *host* is the IP address, hostname, or FQDN of the file server. You must copy and paste the entire key text starting with the hostname, FQDN, or IP address to the end. For example, copy: extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== (ellipses added). **Important** This value must begin with the hostname, FQDN, or IP address that you entered for the Host/IP Address field. For example, if extFileServer is used in the Host/IP Address field, then this field must begin with extFileServer followed by the entire rsa key.
External File Server Directory	The path to the top of the file server directory hierarchy. For example, `/opt/mftFileStore/node_1/`
User Name	The user name of the external file server administrator.

Verify Cisco XCP File Transfer Manager Activation

The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is enabled.

This service can only starts if an external database and an external file server have been assigned, and if the service can connect to the database and mount the file server.

Before you begin

Provision External File Server on IM and Presence Service, on page 14

Procedure

Step 1 On any node in the cluster, log in to the **Cisco Unified IM and Presence Serviceability** user interface.

Step 2 Choose **Tools** > **Service Activation**.

Step 3 From the **Server** drop-down, choose a node where Managed File Transfer is enabled, and click **Go**.

Step 4 Confirm that the **Cisco XCP File Transfer Manager** service's **Activation Status** reads **Activated**.

Step 5 If the service is deactivated, check the **Cisco XCP File Transfer Manager** check box and click **Save**.

Step 6 Repeat this procedure for all cluster nodes where Managed File Transfer is enabled.

What to do next

Enable Managed File Transfer, on page 17

Enable Managed File Transfer

Enable Managed File Transfer on IM and Presence Service.

Procedure

Step 1 Sign in to **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **File Transfer**. The **File Transfer** window opens.

Step 2 In the File Transfer Configuration area, choose either **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer** depending on your deployment. See File Transfer Options, on page 18

Step 3 Enter the Maximum File Size. If you enter 0, the maximum size (4GB) applies.

Note You must restart the Cisco XCP Router service for this change to take effect.

Step 4 In the Managed File Transfer Assignment area, assign the external database and the external file server for each node in the cluster.

a) External Database — From the drop-down list, choose the name of the external database.
b) External File Server — From the drop-down list, choose the name of the external file server.

Step 5 Click **Save**.

After clicking **Save** a **Node Public Key** link, for each assignment, appears.

Step 6 For each node in the cluster that has managed file transfer enabled, you must copy the node's entire public key to the external file server's `authorized_keys` file.

a) To display a node's public key, scroll down to the Managed File Transfer Assignment area and click the **Node Public Key** link. Copy the entire contents of the dialog box including the node's IP address, hostname, or FQDN.

Example:

```
ssh-rsa yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...

...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

(ellipses added).

Warning
- If the managed file transfer feature is configured and the File Transfer Type is changed to either **Disabled** or **Peer-to-Peer**, all managed file transfer settings are deleted.
- A node's keys are invalidated if the node is unassigned from the external database and file server.

b) On the external file server, if it was not left open, open the `~mftuser/.ssh/authorized_keys` file that you created under the *`mftuser`*'s home directory and (on a new line) append each node's public key.

Note The `authorized_keys` file must contain a public key for each managed file transfer enabled IM and Presence Service node that is assigned to the file server.

c) Save and close the `authorized_keys` file.

Step 7 (Optional) Configure the managed file transfer service parameters to define the threshold at which an RTMT alarm is generated for the external file server disk space.

Step 8 Restart the Cisco XCP Router service on all nodes where Managed File Transfer is enabled. See Restart Cisco XCP Router service.

What to do next

Verify External Server Status, on page 18

File Transfer Options

You can configure one of the following file transfer options on the File Transfer window:

File Transfer Option	Description
Disabled	File transfer is disabled for the cluster.
Peer-to-Peer	One-to-one file transfers are allowed, but files are not archived or stored on a server. Group chat file transfer is not supported.
Managed File Transfer	One-to-one and group file transfers are allowed. File transfers are logged to a database and the transferred files are stored on a server. The client must also support managed file transfer, otherwise no file transfers are allowed.
Managed and Peer-to-Peer File Transfer	One-to-one and group file transfers are allowed. File transfers are logged to a database and the transferred files are stored on a server only if the client supports managed file transfer. If the client does not support managed file transfer, this option is equivalent to the Peer-to-Peer option.

Note If managed file transfer is configured on a node and you change the File Transfer Type to **Disabled** or **Peer-to-Peer**, be aware that the mapped settings to the external database and to the external file server for that node are deleted. The database and file server remain configured but you must reassign them if you re-enable managed file transfer for the node.

Depending on your pre-upgrade setting, after an upgrade to IM and Presence Service Release 10.5(2) or later, either **Disabled** or **Peer-to-Peer** is selected.

Verify External Server Status

Verify that there are no problems with the external database setup and with the external file server setup.

Before you begin

Enable Managed File Transfer, on page 17

Procedure

Step 1 To verify the status of the external database:

a) In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External Databases**.

b) Check the information provided in the External Database Status area.

Step 2 On the IM and Presence Service node where you need to verify that the external file server is assigned:

a) In **Cisco Unified CM IM and Presence Administration**, choose **Messaging** > **External Server Setup** > **External File Servers**.

b) Check the information provided in the External File Server Status area to verify that the ceonnection is trouble free.

Troubleshooting External File Server Public and Private Keys

When a server private/public key pair is generated the private key is usually written to `/etc/ssh/ssh_host_rsa_key`

The public key is written to `/etc/ssh/ssh_host_rsa_key.pub`

If these files do not exist, complete the following procedure:

Procedure

Step 1 Enter the following command:

```
$ ssh-keygen -t rsa -b 2048
```

Step 2 Copy the file server's public key.

You must copy the entire string of text for the public key from the hostname, FQDN, or the IP address (for example, *hostname* ssh-rsa AAAAB3NzaC1yc...). In most Linux deployments the key contains the server's hostname or FQDN.

Tip If the output from the `$ ssh-keygen -t rsa -b 2048` command doesn't contain a hostname, then use the output from the following command instead: `$ ssh-keyscan` *hostname*

Step 3 For each IM and Presence Service node that is configured to use this file server, paste the public key into the **External File Server Public Key** field on the **External File Server Configuration** window.

Important Passwordless SSH must be configured for the managed file transfer feature. See the SSHD man page for full configuration instructions for passwordless SSH.

Note While checking the status from the publisher node to the subscriber node, and vice versa the information message "The diagnostics tests for this External File Server may be run from here." is displayed.

In the logs we see "pingable": "-7", which means we are viewing the status of other node where the external file server is not configured.

We configure external file server on the publisher node and the publisher nodes public key is shared in the external file server's "Authorized_key" file.

Administering Managed File Transfer

After you configure Managed File Transfer, you will need to administer the feature on an ongoing basis. For example, you will need to put a system in place for managing file server and database growth. Managed File Transfer Administration Overview.