**Main page:** Cisco Unified MeetingPlace Express, Release 2.x

The Cisco Unified MeetingPlace Express backup and restore functions ensure that the system can recover with minimal data loss in case of a database or system failure or corruption.

# Contents

## About Backing Up the Database

There are three types of database backups:

- L0 (Level 0) backup. This is the most common database backup. This is a complete physical and logical backup of the database from which data can be restored.
- L1 (Level 1) backup. The L1 backup is an incremental backup. It contains a backup of all the data that has been changed since the last L0 backup. It takes much less disk space than an L0 backup; however, it cannot be used for full restoration. If the system fails, you must use both the L0 and L1 backup files to restore data.
- L2 (Level 2) backup. The L2 backup is incremental to the L1 backup, so it needs both the L0 and the L1 backups to restore data.

Cisco Unified MeetingPlace Express uses a combination of L0, L1, and L2 backups and uses an Informix command called **ontape** for the backup mechanism.

The database backup file is physically located on the system disk, which is the same physical device on which the rest of the Cisco Unified MeetingPlace Express system exists. The system disk can contain up to three automatically-created L0 backups: the current L0, plus the previous one or two L0 backups. The L1 and L2 backups are also kept there. All of the older backups are removed from the system disk during the cleanup process.

**Caution!** Use caution if you manually modify the backup files on the local disk or in the archive location. For successful data restoration, the three levels of backup files must be present in the correct order. For example, if the correct L0 and L2 backup files are present while the appropriate L1 backup file is missing, then the data cannot be restored.

You can enable or disable an automatic backup. If the automatic backup is enabled, an L0 backup happens twice a week, every Monday and Thursday at 11:00PM, local server time. The L1 backup is run each day at 1:00AM, local server time, while the L2 backups are done daily at 4:00AM, 8:00AM, 12:00PM, 4:00PM, and 8:00PM, local server time. The schedule is stored in the crontab file.

**Note:** Advanced system administrators can change the frequency of the automatic backups by editing the crontab file. Be careful when modifying the cron schedule, which determines the order of the backups.

The automatic backup process also incorporates archiving (if enabled) and cleanup. This ensures that if there is a database corruption or disk failure, in the worst case, less than four hours of data is lost.

## About Cleaning Up the Database Backup Files

The cleanup process occurs before every scheduled backup in the crontab file. During the cleanup process, the following files are deleted:

- Backup files older than seven days.
- Unusable files, such as L1 and L2 backup files that are older than the oldest remaining L0 backup file.

**Note:** If you disable automatic backups, the cleanup process continues to run as scheduled in the crontab file. Therefore, if you want to keep backup files that are older than seven days, you must archive them.

## Configuring Backups

You can use the Cisco Unified MeetingPlace Express Administration Center to configure the system to automatically back up data. This section describes how to configure the parameters for the automatic backups that the system performs.

**Procedure**

1. Log in to Cisco Unified MeetingPlace Express and click **Administration**.
2. Click **Maintenance > Configure Backup**.
3. Configure the fields on the Configure Backup page.
4. Do one of the following:
   - ♦ To save these values without running the backup program, click **Save**.

♦ To save these values and run the backup process, click **Save and Run Backup**.
♦ To save these values and run the archive process, click **Save and Run Archiving**.

**Related Topics**

- Field Reference: Configure Backup

# Manually Backing Up Data Using the CLI

If you choose to disable the automatic back up feature (by selecting **No** for the Enable automatic backup field on the Configure Backup page), you can still manually back up data.

**Restriction**

- Only run one backup (L0, L1, or L2) at a time.

**Procedure**

1. Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Manually back up the data by entering the following:
   **sudo $MP_DATABASE/db-maintenance/backup.sh <number>**
   where **<number>** is the number of the backup you are running. To make sure you run only one backup at a time, specify 0 for an L0 backup, 1 for an L1 backup, or 2 for an L2 backup. When the system finishes the backup, it displays a "Backup ended" message.
6. On the desktop, click **RedHat > Network Services**.
7. Click **Log out**.

# About Archiving the Database Backup Files and Other External Files

Archiving makes a remote copy of all the backup files and the required external files, such as voice recordings. If a newly archived file has the same name as an existing archived file, the new file overwrites the old file. Maintaining the archive and the remote system used for storing the archive is the responsibility of the system administrator.

**Note:** Backup files and archives do not include backup configuration settings, SNMP configuration settings, SMTP configuration settings, and the custom logo or graphic.

Automatic archiving can be enabled or disabled. When enabled, it is initiated by and happens after the

automatic database backup.

There are two archiving methods:

- rsynch/SSH
- FTP

We recommend that you use the secure SSH/rsync archiving method instead of the FTP archiving method, if possible.

This section contains the following topics:

- About the rsync/SSH Archiving Method
- About the FTP Archiving Method
- About Archiving Recordings

## About the rsync/SSH Archiving Method

The rsync/SSH archiving method is different from the SCP or SFTP archiving methods. It uses the rsync algorithm which is a very fast backup and mirroring tool that synchronizes remote files. It does this by sending just the differences in the files across the link, without requiring that both sets of files be present at one of the ends of the link beforehand.

The remote server to which you archive files must support rsync and SSH connections:

- To archive to a UNIX or Linux server, SSH service and rsync must be enabled on that server. Both SSH service and rsync are included in most UNIX and Linux distributions.
- To archive to a Windows-based server, both an SSH server and an rsync utility must be installed on that server.

## About the FTP Archiving Method

The following restrictions apply to the FTP archiving method:

- The FTP archiving method does not use a secure connection to transfer files to the remote server.
- The FTP archiving method enables the Cisco Unified MeetingPlace Express server to transfer backup files and other critical files to the remote server; FTP clients cannot transfer files to the Cisco Unified MeetingPlace Express server.
- Make sure that the remote host login credentials provide the permissions required to create new directories within in the directory specified in the Pathname location of archive field. For example, if you enter "pub" in the Pathname location of archive field, the following directories are automatically created when the archiving script runs:
    - ♦ pub/compressed_backup
    - ♦ pub/licenses
    - ♦ pub/custom

- Make sure that the FTP remote host user ID and password only contain alpha-numeric characters.
- Occasionally when backing up the system, you might see the Cisco Unified MeetingPlace Express system attempting to log in to the FTP server as an anonymous user. This is most likely caused by special characters in the backup scripts and is not a problem.

### About Archiving Recordings

Because they are external files, meeting recordings and voice recordings of user names are not included in the L0, L1, or L2 backup files. However, meeting recordings are archived and can be restored on your system. Voice recordings of user names are *not* archived and cannot be restored.

End users may also download meeting recordings, rename them, and save them on their PCs. For instructions on downloading meeting recordings, see the User Guide for Cisco Unified MeetingPlace Express Release 2.x.

## Manually Archiving Data Using the CLI

The archive.sh script forces archiving, regardless if auto-archiving is on or off, as set in the procedure described in the Configuring Backups.

**Procedure**

1. Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Manually archive the data by entering the following:
   **sudo $MP_DATABASE/db-maintenance/archive.sh**
   **Note:** The archive.sh script uses remote log-in credentials that are defined in the $MP_DATABASE/db-maintenance/settings.config file. You set these credentials using the procedure described in the Configuring Backups.
   When the system finishes the archive, it displays "Archive ended" and "Archive external files ended" messages.
6. On the desktop, click **RedHat > Network Services**.
7. Click **Log out**.

## Manually Restoring Data Using the CLI

Restoring the data recreates database server data from backed-up storage spaces and logical log files. You may need to restore your data if you need to replace a failed disk that contains database server data, if there is a logic error in a program that has corrupted the database, if you need to move your database server data to a new computer, or if a user accidentally corrupts or destroys data.

The restore is done using the Informix command called **ontape**. Cisco Unified MeetingPlace Express provides a script called restore.sh that guides you through the restore process. The script is in the $MP_DATABASE/db-maintenance directory.

**Restrictions**

- You can only restore a database that is from the same version of the Cisco Unified MeetingPlace Express product. You cannot restore a database from a previous version.
- The names of the databases that you are restoring from and restoring to must be the same.

**Before You Begin**

- To restore data up to the time of the failure, you must have at least one L0 backup.
- You must have the backup files in the correct order. For example, if you have the correct L0 and L2 backup files, but not the appropriate L1 backup file, you cannot restore the data. This requires extra caution if you manually back up files on a local disk or in the archiving location.

**Procedure**

1. Log in to the Cisco Unified MeetingPlace Express operating system as the **mpxadmin** user.
2. At the password prompt, enter the mpxadmin password.
3. Right-click on the desktop.
4. From the menu, select **New Terminal**. This brings up a terminal session.
5. Restore the data by entering the following:
   **sudo $MP_DATABASE/db-maintenance/restore.sh**
6. At the system prompt, press **S** to stop the Cisco Unified MeetingPlace Express application.
7. Choose the type of restore you want. Press **A** for archive or **L** for the local disk.
8. Copy all files from the opt/cisco/meetingplace_express/licenses folder of your latest archive location to the /opt/cisco/meetingplace_express/licenses folder. When finished, press **Enter**.
9. Copy all files from the opt/cisco/meetingplace_express/afs/custom folder of your latest archive location to the /opt/cisco/meetingplace_express/afs/custom folder. When finished, press **Enter**.
10. Copy all files from the mpx-record folder of your latest archive location to the /mpx-record folder. When finished, press **Enter**.
11. The system displays a list of backups that you can restore. Choose one and enter the number associated with it.
12. When prompted, press **R** to perform the restore.
    When the system finishes the archive, it displays the "You restored database successfully" message.
13. On the desktop, click **RedHat > Network Services**.
14. Click **Log out**.