Backing Up and Restoring Data

Last Updated: August 5, 2011

Cisco UMG backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from the Cisco UMG module to the FTP server and the restore function copies the files from the FTP server to the Cisco UMG application. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

We recommend that you back up your configuration files whenever you make changes to the system or application files. Do backups regularly to preserve configuration data.

The system supports the following types of backup:

- All files (backs up configuration and data)
- Only data files (includes dynamic data such as local endpoint IDs, mailboxes, and system distribution lists)

Note We strongly discourage doing the "only data" type of backup and restore because of its potential to introduce inconsistency between configuration and data files.

- Only configuration files (includes the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data)

Two types of backup requests are available: data and configuration only. You can choose one or both.

- Data—Backs up dynamic data such as local endpoint IDs, mailboxes, and system distribution lists.
- Configuration—Backs up system configuration, including the local messaging gateway ID, messaging gateway peers, manually configured endpoints, registration credentials, and NAT data).

Backups are performed only in offline mode. The system displays a message before performing the backup alerting you that the system will be taken offline.

Cisco UMG automatically numbers and dates the backup files. Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3, and the last configuration backup might be 4. Performing an "all" backup might result in a backup ID of 5 for both data and configuration.

When restoring the files, refer to the backup ID for the backup file that you want to use.

Note We recommend that you back up your configuration files whenever changes are made to the system or application files. Data files, which contain voice messages, should be backed up regularly to minimize data loss, such as from a hardware failure.

Restrictions for Backing Up and Restoring Data

- Both the backing up and restoring functions require that the system be in offline mode, so we recommend performing this task when call traffic is least impacted. Offline mode terminates message forwarding and directory exchange.
- Cisco UMG does not support the following backup and restore capabilities:
  - Centralized message storage arrangement. Cisco UMG backup files cannot be used or integrated with other message stores.
  - Selective backup and restore. Only full backup and restore functions are available. Individual messages or other specific data can be neither stored nor retrieved.
- If you delete an endpoint, then do a system restore, the update will erase the information that the endpoint was deleted. You must reset it from the endpoint's primary messaging gateway.