Performing Cisco IPICS Database Backup and Restore Operations

This chapter describes the procedures that you perform to back up your Cisco IPICS database and to restore your database from the backup location.

This chapter includes the following sections:

Overview of Cisco IPICS Database Backup and Restore Operations

As a best practice, Cisco recommends that you back up your Cisco IPICS database on a regular basis and maintain your backups in a secure location. This best practice ensures that you do not lose all system configuration if your Cisco IPICS server experiences a software or hardware failure.

Cisco IPICS performs regularly-scheduled database backups to preserve your data. For more information about scheduled database backups, including the default settings for the scheduled database backups and how to modify them, see the "Changing the Default Settings for a Scheduled Database Backup" section on page 9-9.

You can also perform a database backup at any time by manually executing the backup operation. For more information about manual backup procedures, see the "Restoring Data from a Database Backup" section on page 9-12.

After you have backed up your data, you can restore your data by choosing from various options. By accessing the **Administration > Database Management** window, you can identify the backup that you want to restore. For more information regarding restore operations, see the "Restoring Data from a Database Backup" section on page 9-12.

Backing up the Cisco IPICS Server Database

Cisco IPICS provides you with the following options to back up your database:

- Manual backups—You can perform a manual database backup to capture the current state of the Cisco IPICS database.
- Scheduled backups—By default, Cisco IPICS backs up the database every day at a predefined time and stores the backup in a predefined location. You can change the time, frequency, and/or location of the scheduled backup.

This section includes information about backing up the database and includes the following topics:

Managing Database Backups from the Database Management Window

To configure the parameters for backing up your database, and performing backup-related operations, navigate to the **Administration > Database** Management window.

The Database Management window includes the following tabs:

- Database Backup—From this tab, you can configure the options to back up your database. See the "Performing a Manual Database Backup" section on page 9-3 for more information about the Database Backup tab.
- Restore From Backup—From this tab, you can restore your database backup. See the "Restoring Data from a Database Backup" section on page 9-12 for more information about restoring your database backup.
- Schedule Backup—From this tab, you can configure the options that apply to regularly-scheduled backups. You can specify the location of the backup and the length of time for which the backup is saved. In addition, you can specify when, and how often, Cisco IPICS performs the scheduled backups.

  See the "Changing the Default Settings for a Scheduled Database Backup" section on page 9-9 for more information about changing the settings for the scheduled database backups.
- Log—From this tab, you can view the database logs, which include backup and restore activity. The logs include status messages and information about any errors that might have occurred during a database backup or restore procedure. See the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19 for more information about the database logs.

Performing a Manual Database Backup

To perform a manual database backup, navigate to the **Administration > Database Management > Database Backup** window.

The settings that you choose for a manual database backup, such as the location of the backup, can be different from the destination that you choose for the scheduled backups. (Settings for manual database backups do not affect or change the settings for scheduled database backups.)

To manually back up the database, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Database Backup** window.

Step 2 In the **Backup Destination** pane, choose one of the following destinations:

- **Default**—Click this radio button to place the backup in the default (**/idspri/backup**) directory.

  Cisco IPICS creates a subdirectory in the /idspri/backup directory for the database backup named **IDSB**_*yyyy-mm-dd_hh-mm-ss*. See the "Understanding Naming Conventions for Backup Directories" section on page 9-8 for more information about backup directory naming conventions.

- **Local Directory**—Click this radio button to specify a directory in the Cisco IPICS server to back up your database.

Note Cisco IPICS prepopulates the Local Directory field with the **/idspri/backup** directory. If you back up your files to a local directory in the server, that directory must be a subdirectory of the **/idspri/backup** directory. Any directory within the **/idspri/backup** directory (for example, **/idspri/backup/mybackups**) is valid as a location for a database backup. If the directory that you specify does not exist, Cisco IPICS creates the directory for you.

Make sure that you enter the path within the **/idspri/backup** directory in the Cisco IPICS server, and that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays a pop-up window with an error and does not perform the backup.

- **Remote Host**—Click this radio button to back up your database to a remote location.

Note Use the Remote Host option only if the remote host supports the Linux Secure Copy (scp) command. If you are using a remote host that does not support scp (for example, a Windows PC or server), click the **Local Directory** radio button. You must back up your data to the Cisco IPICS server, then use a secure file transfer protocol (SFTP) client software program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. For more information, see the procedure in the "Backing Up Data to a Remote Host Without scp Support" section on page 9-31 to back up your files to a remote host that does not support scp.

When you click the Remote Host radio button, you must specify the following information:

- Remote Host IP Address—Enter the IP address of the remote host.
- User Name—Enter a valid user name for access to the remote host.
- User Password—Enter a valid password for this user.
- Remote Directory—Enter the location of the full directory path on the remote host where you want the database to be stored. If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.

  For more information, see the "Caveats for Remote Host Database Backups" section on page 9-11.

Step 3 Click **Backup Now**.

Cisco IPICS begins the database backup process. An information icon appears in the tab to inform you that the backup is in process, along with the following text:

```
Database backup in progress. Please wait...
```

Step 4 To view the activity for the backup, wait a few moments for the screen to refresh and view the Backup Log pane.

The Backup Log pane in the Database Backup tab displays the log entries for the backup process. The screen refreshes periodically with log messages until the database backup completes.

Note To manually refresh the screen, click **Refresh**.

Step 5 To view the results of the backup operation, wait until the screen stops refreshing, then view the Backup Log pane.

Note The backup log pane can contain multiple pages of items. To view items in the list, use the navigation buttons as described in the "Navigating Item Lists" section on page 1-15.

If the backup operation was successful, you see a Status Text of **Available**.

Table 9-1 describes the fields in the Backup Log pane.

Table 9-1 Field Descriptions in the Backup Log Pane

Field	Description
ID	This field represents the internal ID of the database backup. Cisco IPICS gives each backup operation a unique ID.
Backup Destination	This field represents the full directory path of the database backup, beginning with a forward slash (/). If the backup was a Remote Host backup, this field displays the full directory path on the remote server on which Cisco IPICS placed the Remote Host backup. **Note** Cisco IPICS creates a subdirectory inside the directory that you specify for each backup operation. Each directory is time-stamped with the date and time of the backup, as described in the "Restoring Data from a Database Backup" section on page 9-12.
IP Address	This field represents the IP address of the remote server, if the backup was a Remote Host backup. If Cisco IPICS performed a Default or Local Directory backup, this field is blank. If the backup operation was not successful, this field displays **none**.

Table 9-1 Field Descriptions in the Backup Log Pane (continued)

Field	Description
Status	This field represents the status of the backup operation. The status field displays one of the following states: • **Initialized**—The backup process has begun the initial stages of the database backup. • **In Progress**—Cisco IPICS successfully completed the initial stages of the backup process and is performing the database backup. • **Available**—The database backup was successful and the specified backup is available for a restore operation. • **Not Available - Purged**—The specified database backup exceeded the retention period as specified by the **Backup Retention** list box and Cisco IPICS deleted the database backup. The date and time that the database was purged is displayed in the field. • **Canceled**—Cisco IPICS canceled the backup due to a known error (for example, a lack of hard disk space). • **Failed**—Cisco IPICS could not complete the database backup because of an unexpected error. If you see a **Canceled** or **Failed** error status, your database backup failed. You can find more information about the cause of the failure by navigating to the **Administration > Database Management > Log** window and viewing the contents of the backup log.
Size in Bytes	This field represents the total size, in bytes, of the specified database backup.
Backup Start Time	This field represents the time that Cisco IPICS started the specified database backup.
Backup End Time	This field represents the time that Cisco IPICS completed the specified database backup.
Purge Time	This field represents the time that Cisco IPICS deleted the specified database backup.

You can also view the database logs by navigating to the **Administration > Database Management > Logs** window. To visually identify the type of status message that appears in the Database Logs pane, Cisco IPICS displays certain log entries in the following text colors:

- Green—Green messages indicate the completion of a script.

Note Carefully check the text of green messages to ensure that the script completed successfully with no errors. Green messages do not indicate whether the script completed successfully.

- Black—Black messages are informational messages, and indicate normal database backup processes.
- Blue—Blue messages are warning-level messages, and indicate problems that are less severe than error-level messages, such as a backup operation that completed with errors. Occasionally a warning-level error message can indicate a greater problem, such as a restore operation that did not complete successfully.
- Red—Red messages are error-level messages, and indicate that a process did not complete successfully. Red messages usually indicate errors of a greater severity than warning-level (blue) messages.

For more information about troubleshooting problems that you might encounter, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 9-30.

Understanding Naming Conventions for Backup Directories

Cisco IPICS creates a subdirectory in the backup directory for each database backup. Cisco IPICS time-stamps each subdirectory with the date and time that Cisco IPICS performed the backup operation. The subdirectory name is in the following format:

IDSB_*yyyy-mm-dd_hh-mm-ss*

Where *yyyy-mm-dd_hh-mm-ss* represents the year, month, day, hour, minute and second, respectively, of the time that the Cisco IPICS performed the database backup (for example, IDSB_2006-09-04_17-13-55).

Changing the Default Settings for a Scheduled Database Backup

Cisco IPICS is preconfigured with default settings for database backups. Table 9-2 shows the default settings for scheduled database backups:

Table 9-2 Default Settings for Scheduled Database Backups

Setting	Value
Frequency	Daily
Time of day	23:59 (11:59 p.m.)
Destination directory	The Cisco IPICS server **/idspri/backup** directory. This directory displays as part of the Local Directory option.
Backup retention	8 days

You can modify any of the default settings that are displayed in Table 9-2. Your changes become effective only after you click Save and they become the default settings.

To modify the automated settings for a database backup, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Schedule Backup** window to access the Schedule Backup tab.

Step 2 In the **Schedule Destination** pane, choose from one of the following destinations for your database backup:

- **Default**—Click this radio button to place the database backup in the **/idspri/backup** directory.
- **Local Directory**—Click this radio button to specify a subdirectory of the **/idspri/backup** directory on the local server to back up your database. If you backup your files to a local directory on the server, that directory must be a subdirectory of the **/idspri/backup** directory. If the directory does not exist, Cisco IPICS creates the directory for you.

Note Make sure that you precede the destination path with a forward slash (/). If you do not specify a forward slash, Cisco IPICS displays an error message in the **Administration > Database Management > Log** window and does not perform the database backup.

- **Remote Host**—Click this radio button to back up your database to a remote location. When you choose this option, you must specify the following information:
  - Remote Host IP Address—Enter the IP address of the remote host.
  - User Name—Enter a valid user name for access to the remote host.
  - User Password—Enter a valid password for this user.
  - Remote Directory—Enter the location of the full directory path on the remote host where you want the database to be stored.

See the "Choosing a Destination for the Database Backup" section on page 9-11 for more information about choosing a destination, user name, and password for your backup.

Step 3 To change the retention settings for the database backup, click the **Backup Retention** drop-down list box to choose the number of days that you want the database to be stored.

Cisco IPICS deletes any backup files that are older than the backup retention setting whenever it performs a scheduled or manual backup.

Note Cisco IPICS does not purge Remote Host backups.

Step 4 In the **Schedule Time** pane, view the default time and day values for the scheduled backup and, if required, modify the values by performing the following steps:

a. Modify the time of day for the scheduled backup to begin by clicking the **Start Time** drop-down list boxes and choose the appropriate values.

b. Under **Repeat Every**, modify the frequency of the scheduled backups by clicking the radio button that corresponds to one of the following options:
   - **Day**—This option schedules a daily backup. Click this radio button to configure daily database backups.

- **Specific Days**—This option activates the check boxes for individual days of the week. Click this radio button and check the appropriate days of the week to perform a database backup on the days of the week that you select.

Step 5 Click **Save** to apply and save your changes.

Caution If you do not click **Save**, your changes are not saved and the server reverts to the current default settings.

To discard your changes and return to the current default settings, click the **Cancel** button.

Choosing a Destination for the Database Backup

When you specify the options for a scheduled database backup, or when you perform a manual backup, you should determine the best place to store the backup. For more information, refer to the "Guidelines for Choosing a Destination for Database Backups" section in the *Release Notes for Cisco IPICS Release 2.0(1)*.

Caveats for Remote Host Database Backups

When you specify the Remote Host option, be aware of the following caveats:

- You must know the IP address of the remote host.
- You must use a valid user name and password on the remote host.
  - The user name for the remote host is not encrypted in the Cisco IPICS server and is stored as clear text. Therefore, Cisco recommends that you create a special user name that has restricted access to the remote host, has scp access, and has write access to only the directory to where you save the database backup.
  - To help ensure the security of your data, Cisco IPICS does not support the use of different user IDs for remote backup and restore operations that you perform on the same data set. Therefore, when you restore your

data, make sure that you specify the same user ID as the one that you used to back up your data. If you specify a different user ID, the restore procedure does not succeed because of file accessibility issues; in this situation, Cisco IPICS displays "permission denied" error messages in the db-maintenance.log. As a best practice, Cisco recommends that you designate a specific user ID that you can use for all of your remote backup and restore activities.

- The remote host that you specify must be capable of running the scp command. If there are no remote hosts on your network that support scp (for example, a Windows PC or server), use the Local Directory option to back up your data, then use an SFTP client program, such as SSH Secure Shell Client software (or similar software), to copy the backup files to a remote host. Follow the procedure in the "Backing Up Data to a Remote Host Without scp Support" section on page 9-31 to back up your data to a remote host that does not support scp.
- If the directory that you specify for the backup does not exist on the remote host, Cisco IPICS creates it for you.

Restoring Data from a Database Backup

When you perform a restore operation, you retrieve data from a database backup, and restore the Cisco IPICS database to the state that it was in at the time that Cisco IPICS performed the backup.

You may need to restore your database if you encounter one or more of the following situations:

- You have to reinstall the server software and you need to restore the database to the state that it was in before you reinstalled the software.
- Server data, such as channels, channel groups or VTG templates, were deleted from the database in error and you need to retrieve them.
- You need to copy a database from one Cisco IPICS server to another Cisco IPICS server. You copy the database by performing a database backup from one server, and restoring the database from that backup to another server.

Note You can restore data from one server to another only if both servers are using the same version of Cisco IPICS software. If the software versions of the two servers differ, the database schema might not be the same. In this case, the restore operation fails.

This section contains information about restoring your data and includes the following topics:

Options for Using the Restore Procedure

To configure the restore parameters and perform all restore operations, access the **Administration > Database Management > Restore from Backup** window.

Caution A restore operation logs all users out of the Cisco IPICS database and users cannot log in to Cisco IPICS until the restore operation completes. To minimize any disruption that the restore procedure may cause to users, Cisco recommends that you perform a restore operation during a maintenance window or other off-peak hours.

You can restore your data from the default location, from another local directory that you specify, or from a remote host.

Note Before you restore your database, be aware that any configuration changes that you made to the server after Cisco IPICS performed the database backup are not restored to your server by the restore operation. If you want to ensure that all your recent configuration changes are restored, perform another database backup before you perform the restore operation. For more information, see the "Backing up the Cisco IPICS Server Database" section on page 9-2.

Performing the Restore Procedure

To restore your data, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Restore from Backup** window.

Step 2 In the **Restore Destination** pane, choose from the following options to restore your data:

- **Default**—Click this radio button to restore your data from the default location, which is **/idspri/backup**. If you backed up your database in the default location, choose this option. If there is more than one database backup in the default directory (for example, if you perform regularly scheduled database backups), Cisco IPICS uses the most recent backup for the restore operation.
- **Local Directory (requires full path)**—Click this radio button to restore your data from the local directory that you specify.

  When you specify a local directory or remote host for your restore operation, make sure that you specify the entire directory path. Make sure that you include the following directories in the directory path:

  - The **/idspri/backup** directory. Cisco IPICS places every backup to a local directory in the **/idspri/backup** directory
  - The **IDSB**_*yyyy*-*mm*-*dd*_*hh*-*mm*-*ss* directory that Cisco IPICS created when it performed the database backup.

  Note You also specify the Local Directory option if you backed up your data to a remote host that does not support scp. If you backed up your files to a remote host that does not support scp, follow the procedure in the "Restoring Data from a Remote Host Without scp Support" section on page 9-32 to move the backed-up files from the remote host to a local directory. Then, continue with this procedure.

- **Remote Host**—Click this radio button to restore your data from a remote host, in the directory location that you specify.

When you click the Remote Host radio button, you must specify the following information:

- Remote Host IP Address—Enter the IP address of the remote host.
- User Name—Enter a valid user name for access to the remote host.

  Your data is more secure if the same user performs both the backup and restore operations; therefore, the user name to restore the data must be the same user name that you used to back up the database. If you specify a different user name, the restore procedure does not succeed because the user does not have the correct permissions to access the backed-up database.
- User Password—Enter a valid password for this user.
- Remote Directory—Enter the directory path for the remote host from which you want the database to be restored. Enter the full directory path, including the directory that was generated by Cisco IPICS for the database backup, for example **/mybackups/IDSB_2006-08-25_17-13-55**.

Note Be sure to enter the correct user name, password, and remote directory; otherwise, the scp process fails. If the scp process fails, you can determine the cause of the failure by checking the logs in the **Administration > Database Management > Log** window.

Step 3 Click **Restore Now**.

A pop-up window displays to confirm the restore process.

Note If you confirm the restore process, all of the data that has been saved since the last time that your data was backed up, is lost. If you want to cancel the restore process and retain the data that has been saved since the last backup, click **Cancel**.

Step 4 Click **OK**.

Cisco IPICS begins the restore process and logs all users out of the Administration Console.

Note Unlike a database backup operation, you cannot view the log details of the restore operation while it is in progress. The Tomcat service restarts during the restore operation and automatically logs all users out of Cisco IPICS. You must wait for the restore process to complete before you can log in again. You can check the status of the restore process in the **/opt/cisco/ipics/database/logs/db-maintenance.log** file on the Cisco IPICS server. For more information, see the "Checking the Restore Status in the Database Log" section on page 9-17.

Step 5 To see the status of the restore operation, perform one of the following actions:

- To view the status of the restore operation by using CLI commands, see the "Checking the Restore Status in the Database Log" section on page 9-17. The use of CLI commands allows you to see the status of the restore operation before you are able to log back in to the server.
- To view the final status of the restore operation, perform the following procedure:

  a. Wait about 10 to 15 minutes, then log in to the Administration Console by using the ipics user ID.

  If you attempt to log in to the Administration Console before the restore process completes, Cisco IPICS displays the following message:

  ```
  You entered an invalid user name or password.
  Please try again.
  If this problem persists, the database may be unavailable.
  Contact your System Administrator for help.
  ```

  If you receive the preceding message, you can check the progress of the restore operation by opening a terminal window and checking the log as described in the "Checking the Restore Status in the Database Log" section on page 9-17. If you continue to be unable to log in, follow the troubleshooting procedures in the "Unable to Log In To the Administration Console After Restoring Data" section on page 9-34 to attempt to fix the problem.

  b. Navigate to the **Administration > Database Management > Log** window.

  c. Check the Database Logs pane to view the most recent status messages regarding the restore procedure.

Note Click **Refresh** to refresh the log window and view new messages.

Step 6 To view the entire database log file, perform the following procedure:

a. Wait approximately 20 minutes and then log in to the Administration Console.

b. Navigate to the **Administration > Database Management > Log** window.

c. Click **Download**.

d. Perform the actions as listed in Step 3 in the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19 to unzip the .zip file and view or download the db-maintenance.log file.

Checking the Restore Status in the Database Log

Cisco IPICS logs out all users from the Cisco IPICS Administration Console when the restore process begins. You cannot log in to the Administration Console until the process completes. To check the status of the restore procedure before it completes, log in to the Cisco IPICS server and view the contents of the db-maintenance.log file.

The db-maintenance.log file is located in the following directory on the server: **/opt/cisco/ipics/database/logs**. For more information about the db-maintenance.log file, and other log files in Cisco IPICS, see the "Downloading and Viewing the Backup and Restore Logs" section on page 9-19.

To manually access the database log and check the status of the restore operation, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the ipicsadmin user ID.

- From a direct server connection, log in by using the ipicsadmin user ID.
- From a remote secure client, open a terminal window using SSH Secure Shell Client software or similar software. Then, log in by using the ipicsadmin user ID.

A terminal window displays.

Note The ipicsadmin user has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. You can also use the root user ID to perform this procedure.

Step 2 Enter the following command to see the last 25 lines of text in the db-maintenance.log file:

[ipicsadmin]# **tail -25 /opt/cisco/ipics/database/logs/db-maintenance.log**

The last 25 lines of the log file displays. If the log file contains less than 25 lines, the entire file displays.

Step 3 Check the last lines of the db-maintenance.log file to see whether the restore process completed successfully.

Step 4 To check the status of the restore operation, perform one or more of the following actions, depending on the output in the db-maintenance.log file:

- If you see the "Restore process ended without errors" log entry, the restore process completed successfully and no further action is required.
- If you do not see the "Restore process ended without errors" log entry, or if you do not see any other message that indicates that the restore process has completed, wait several minutes and then repeat Step 2.
- If you see an error message indicating that the restore process ended but was not successful, check the log files by performing the following procedure:

  a. Enter the following command:

  [ipicsadmin]# **more /opt/cisco/ipics/database/logs/db-maintenance.log**

  Press the Spacebar to see additional lines of text, if necessary.

  b. View and evaluate the log file entries.

  The log file should give an indication as to why the restore process did not complete successfully. For example, if you performed a backup to a remote host and specified a user name that does not have the proper permissions to perform an scp operation, a message similar to the following example displays:

```
2007-01-16 15:10:21 Error: Remote scp failed because of a
password error on host: 10.1.1.1 User: invalidscpuser
```

c. Note the failure that occurred.

d. Perform any actions as indicated by the failure to fix the problem. If you require further assistance, see the "Troubleshooting Cisco IPICS Backup and Restore Procedures" section on page 9-30 to attempt to fix the problem.

e. Retry the restore operation by following the procedure in the "Performing the Restore Procedure" section on page 9-14.

Downloading and Viewing the Backup and Restore Logs

Cisco IPICS stores the logging details of backup and restore activity in two files, db-maintenance.log and dbm_log_archive.log.gz.

- The db-maintenance.log file captures the logging information that Cisco IPICS generates for backup or restore operations in a single day. Cisco IPICS saves the log information for the day that it last performed a backup or restore operation in the db-maintenance.log file.

  You can view the contents of the db-maintenance.log file in the **Administration > Database Management > Log** window.

Note The db-maintenance.log file does not exist on the server until you perform a database backup or restore operation for the first time.

- The dbm_log_archive.log.gz file is a compressed file that contains archived data from previous db-maintenance.log daily log files.

  Whenever you perform a backup or restore operation, Cisco IPICS checks the db-maintenance.log file to see if it contains log data for that day. If the db-maintenance.log file contains data for a previous day, Cisco IPICS moves

the information in the db-maintenance.log file to the dbm_log_archive.log.gz file. Cisco IPICS then saves the log data from the current backup or restore operation to the db-maintenance.log file.

The default maximum allowable size of the dbm_log_archive.log.gz file is 5 MB. When the file reaches the maximum size, Cisco IPICS removes 5 percent of the oldest information in the dbm_log_archive.log.gz file until the file is smaller than the configured maximum size.

You can download the dbm_log_archive.log.gz file, along with the db-maintenance.log file, and save it to your PC by clicking the **Download** button in the **Administration > Database Management > Log** window. Once you download the files to your PC, you can view them as a text file.

Note The downloaded files are joined and compressed into a single zipped file. The machine to which you download the zipped file must have an application, such as WinZip, installed to be able to open and extract the files.

To download the db-maintenance.log and the database archive file from the Administration Console, perform the following procedure:

Procedure

Step 1 Navigate to the **Administration > Database Management > Log** window to access the Log tab.

Step 2 Click **Download** to open the Download dialog box.

The Download dialog box displays.

Step 3 Click **Save** to save the compressed file to your PC.

The **Save As** dialog box opens.

Step 4 Navigate to the directory location where you want to save the file; then, click **Save**.

The download program saves the .zip file to the location that you specified.

Step 5 Navigate to the directory location where you saved the .zip file.

Step 6 Double-click the .zip file to open it.

The .zip file opens and displays the db-maintenance.log and dbm_log_archive.log.gz files.

Step 7 Click **Extract**.

The Extract window opens.

Step 8 Navigate to the location of the directory where you want to save the log files.

Step 9 Click **Extract**.

The extract program saves the log files to the location that you specified on your PC.

Step 10 To view the content of the log files, open the files with any software program that allows you to view text files.

Using CLI to Export and Import the Cisco IPICS Databases

In some situations, you may not be able to back up and restore your data by using normal backup and restore operations.

The following examples represent situations when you cannot use the backup and restore functionality in the Administration Console.

- A hardware error rendered your browser inoperable, and you cannot access the Cisco IPICS Administration Console. However, you can still access the database files by using CLI commands.
- You need to upgrade your system to a later version of the Cisco IPICS operating system and Cisco IPICS software. The database schema might be different between the Cisco IPICS software releases. In this situation, you would export your data to an external source, load the newest release of Cisco IPICS operating system (if required) and Cisco IPICS software onto the server, and import the data to the current release of Cisco IPICS.

To perform backup and restore operations without using the Administration Console, or migrate your data to a later version of Cisco IPICS, use the CLI-based import and export script utilities. To manually perform this functionality, use the **export_ipics_db** utility program to back up your databases, and the **import_ipics_db** utility program to restore your databases.

This section describes the import and export procedures and includes the following topics:

Understanding the Cisco IPICS Databases

Cisco IPICS has four databases. See Table 9-3for a description of the databases.

Table 9-3 Cisco IPICS Databases

Database Name	Description
ipics	This is the primary database for the Cisco IPICS application.
ippe	This is the database for the policy engine.
db_cra	This is the primary database for the dial engine. It contains the dial engine configuration including the following: • SIP provider configuration • Dial engine application definitions (for example, an instance of a dial engine script with an associated trigger) • Application triggers (for SIP and HTTP) • System configuration parameters
db_cra_repository	This is the script and prompt database for the dial engine. The following elements are stored in this database: • Standard dial engine scripts (in *.aef format) • Custom dial engine scripts (in *.aef format) • Standard script prompts (in *.wav format) • Customized script prompts (in *.wav format) • Spoken names (in *.wav format)

Using the Database Export Utility

The **export_ipics_db** utility program backs up your database, and creates the ipics.exp directory and the dbexport.out file.

Before you run the export utility, you must create a subdirectory for each of the four databases. If you do not create a separate subdirectory for each database, the export utility overwrites any export files that exist in the directory.

Note When you perform an upgrade from Cisco IPICS release 1.0(2) to release 2.0(1), you only export the ipics database. The ipics database is the only database that exists in Cisco IPICS release 1.0(2).

You can run the export utility program as often as you require. You create a directory for each export operation. Cisco recommends that you name the subdirectory of each backup set to include a date so that you can easily identify it.

To use the export utility, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server by using the root user ID.

- From a direct server connection, log in by using the root user ID.
- From a remote secure client, open a terminal window using SSH Secure Shell Client software or similar software. Then, log in by using the root user ID.

  A terminal window displays.

Step 2 If it does not already exist, create a main directory for your export by entering the following command:

[root]# **mkdir -p /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>

where:

<*subdirectory_name*> is the name that you specify to identify this backup set. Cisco recommends that you include the day and month of the backup, for example **ipics_backup_02_07_2007**.

Step 3 Navigate to the directory that you just created by entering the following command:

[root]# **cd /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>

Step 4 Create a subdirectory for the ipics database export operation by entering the following command:

[root]# **mkdir ipics**

Step 5 If you are performing an export from Cisco IPICS release 2.0(1), create subdirectories for the three additional databases that exist in release 2.0(1) by performing the following steps:

a. Create a subdirectory for the ippe database export operation by entering the following command:

[root]# **mkdir ippe**

b. Create a subdirectory for the db_cra database export operation by entering the following command:

[root]# **mkdir db_cra**

c. Create a subdirectory for the db_cra_repository database export operation by entering the following command:

[root]# **mkdir db_cra_repository**

Note If you are performing an upgrade from Cisco IPICS release 1.0(2) to 2.0(1) you do not need to perform this step, as the ipics database is the only one that exists in Cisco IPICS release 1.0(2).

Step 6 Make sure that the informix user and the ipics group own the **/idspri/backup/IPICS_BACKUPS** directory and its subdirectories by entering the following command:

[root]# **chown -R informix:ipics /idspri/backup/IPICS_BACKUPS**

Step 7 Log in as the informix user by entering the following command:

[root]# **su - informix**

Step 8 Navigate to the export directory by entering the following command:

[informix]# **cd /idspri/backup/IPICS_BACKUPS/<***subdirectory_name***>**

Step 9 Navigate to the ipics subdirectory by entering the following command:

[informix]$ **cd ipics**

Step 10 Execute the export utility program and export the ipics database by entering the following command:

[informix]$ **export_ipics_db ipics**

Cisco IPICS displays the following message on the console:

```
WARNING: This action will bring the database server to Single-user
mode - Confirm?([Y]/N):
```

Step 11 Enter **Y** to confirm the database export operation.

Cisco IPICS backs up your primary ipics database and places the contents in the ipics.exp subdirectory.

Step 12 If you are performing an upgrade procedure from Cisco IPCS release 1.0(2) to Cisco IPICS 2.0(1), perform the following steps:

a. Copy the information in the ipics directory to an external host.

b. Install the Cisco IPICS operating system software and server software.

c. Perform the import procedure as described in the "Using the Database Import Utility" section on page 9-26.

Step 13 If you are performing an export procedure from Cisco IPICS release 2.0(1), perform the following steps:

a. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

b. Navigate to the ippe subdirectory by entering the following command:

[informix]$ **cd ippe**

c. Export the ippe database by entering the following command:

[informix]$ **export_ipics_db ippe**

Cisco IPICS displays the following message on the console:

```
WARNING: This action will bring the database server to Single-user mode - Confirm?([Y]/N):
```

d. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the database for the policy engine and places the content in the ipics.exp subdirectory.

e. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

f. Navigate to the db_cra subdirectory by entering the following command:

[informix]$ **cd db_cra**

g. Export the db_cra database by entering the following command:

[informix]$ **export_ipics_db db_cra**

h. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the dial engine database.

i. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

j. Navigate to the db_cra_repository subdirectory by entering the following command:

[informix]$ **cd db_cra_repository**

k. Export the db_cra database by entering the following command:

[informix]$ **export_ipics_db db_cra_repository**

l. Enter **Y** to confirm the database export operation.

Cisco IPICS backs up the script and prompt database for the dial engine.

Using the Database Import Utility

After you save the exported backup files to a new or existing server, you run the **import_ipics_db** utility program for each database. This utility program imports the backed-up content and rebuilds the databases on your server.

You can run the import utility program from any Cisco IPICS installation. If you have several backup sets from which to restore, be sure to run the import utility program from the subdirectory that contains the specific backup set that you want.

Procedure

Step 1 Open a console terminal or remote terminal window, and log in by using the root user ID.

Step 2 Stop the database processes by entering the following command from the command prompt:

[root]# **service ipics stop**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the **service ipics stop** command. For more information about the policy engine, refer to the "Using the Cisco IPICS Policy Engine" chapter of the *Cisco IPICS Server Administration Guide*.

Step 3 Navigate to the **/idspri/backup/IPICS_BACKUPS** directory by entering the following command:

[root]# **cd /idspri/backup/IPICS_BACKUPS**

Step 4 If you have several backup sets in this directory, find the subdirectory for the backup set that you want to restore by entering the following command:

[root]# **ls -l**

Step 5 Navigate to the subdirectory that contains the backup set that you want to restore by entering the following command:

[root]# **cd** <*subdirectory_name*>

where:

<*subdirectory_name*> is the name of the subdirectory that contains the backup set.

Step 6 Navigate to the ipics subdirectory by entering the following command:

[root]# **cd ipics**

Step 7 Verify that the ipics.exp directory exists in this subdirectory by entering the following command:

[root]# **ls -l**

The following information displays:

```
[informix]$ ls -l
total 120
-rw-r-----    1 informix ipics 110699 Oct 23 16:26 dbexport.out
drwxr-x---    2 informix ipics 4096 Oct 23 16:26 ipics.exp
```

Step 8 Enter the following command to retrieve the full path of the directory that contains the backup set:

[root]# **pwd**

Step 9 Make a note of the full directory path that displays.

Step 10 Log in as the informix user by entering the following command:

[root]# **su - informix**

The server logs you in as the informix user and places you in the /home/informix directory.

Step 11 Navigate to the directory in which the ipics.exp directory is located by entering the following command:

[informix]$ **cd /idspri/backup/IPICS_BACKUPS/**<*subdirectory_name*>**/ipics**

where:

<*subdirectory_name*> is the name of the subdirectory that contains the backup set.

Step 12 Execute the import utility program by entering one of the following commands, depending on the release of Cisco IPICS from which the database was exoirted:

- If the data was exported from Cisco IPICS release 1.0(2), enter the following command:

  [informix]$ **import_ipics_db ipics -convert**

- If the data was exported from Cisco IPICS release 2.0(1), enter the following command:

  [informix]$ **import_ipics_db ipics -drop_db**

Step 13 Enter **Y** to confirm the database import operation.

If you are upgrading from Cisco IPICS release 1.0(2), Cisco IPICS converts the 1.0(2) database schema to the 2.0(1) database schema, and restores your primary ipics database. If you are importing data from Cisco IPICS release 2.0(1), Cisco IPICS drops the existing database in your server, and imports the imported database to your server.

Step 14 If you are upgrading from Cisco IPICS release 1.0(2), proceed to Step 15. If you are restoring a database set from Cisco IPICS release 2.0(1), perform the following steps:

a. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

[informix]$ **cd ..**

b. Navigate to the ippe subdirectory by entering the following command:

[informix]$ **cd ippe**

c. Execute the import utility program and import the ippe database by entering the following command:

   [informix]$ **import_ipics_db ippe -drop_db**

   Cisco IPICS restores the database for the policy engine.

d. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported database for the policy engine.

e. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

   [informix]$ **cd ..**

f. Navigate to the **db_cra** subdirectory by entering the following command:

   [informix]$ **cd db_cra**

g. Execute the import utility program and import the ippe database by entering the following command:

   [informix]$ **import_ipics_db db_cra -drop_db**

h. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported dial engine database.

i. Return to the parent backup directory <*subdirectory_name*> by entering the following command:

   [informix]$ **cd ..**

j. Navigate to the **db_cra_repository** subdirectory by entering the following command:

   [informix]$ **cd db_cra_repository**

k. Execute the import utility program and import the **db_cra_repository** database by entering the following command:

   [informix]$ **import_ipics_db db_cra_repository -drop_db**

l. Enter **Y** to confirm the database import operation.

   Cisco IPICS drops the current database, and imports the exported script and prompt database for the dial engine.

After the import process is complete, you must restart the Tomcat service to synchronize the information in the database and the RMS.

Step 15 To restart the Tomcat service, follow these steps:

a. Enter **exit** to log out of the informix user ID.

b. Enter the following command to restart the Tomcat service and the policy engine:

[root]# **service ipics restart**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the service **ipics restart** command.

Cisco IPICS displays the `[OK]` message after the Tomcat service has successfully stopped, and again after it has successfully restarted.

If the Tomcat service does not successfully start, refer to the *Cisco IPICS Troubleshooting Guide, Release 2.0(1)* for more information.

There may be a slight delay before users can access the Administration Console after the Tomcat service restarts.

Troubleshooting Cisco IPICS Backup and Restore Procedures

This section describes how to troubleshoot backup and/or restore activity.

The procedures that are described in this section require that you have access to one or more of the following user IDs:

- root
- informix
- ipicsadmin

This section includes the following topics:

Backing Up Data to a Remote Host Without scp Support

Problem The remote host to which you want to back up your data does not support the scp command (for example, if the remote host is a Windows PC or server).

Solution Choose the Local Directory option when you back up your files, then use an SFTP client software program to copy your backup data to a remote host.

Perform the following procedure to back up your data to a remote host that does not support scp:

Procedure

Step 1 Back up your files to a local directory by following the procedure in the "Performing a Manual Database Backup" section on page 9-3.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you are using SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 5 In the User Name field, enter **root**.

Step 6 Click **Connect**.

The Enter Password window displays.

Step 7 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the server and displays the contents of the **/root** directory in the right pane of the window.

Step 8 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 9 In the **Enter Folder Name** field, enter the name of the folder where you backed up your files (for example, **/idspri/backup/mybackup**).

The right pane of the window displays the contents of the folder. The folder contains a directory that is timestamped with the date and time that the local directory backup was performed, for example **IDSB2006-11-02_14-04-52**. This directory contains your backup files.

Step 10 In the left pane of the window, navigate to the folder on your PC where you want to copy the backup files.

Step 11 Click the timestamped **IDSB***yyyy-mm-dd_hh-mm-ss* folder in the right pane of the window.

Step 12 Drag the folder from the right pane of the window to the left pane to initiate the copy procedure.

A progress window displays while the file copies the backup folder to the folder that you specified on your PC. When the copy completes, the backup folder displays in the left pane.

Step 13 Close the SSH Secure Shell File Transfer Client.

Restoring Data from a Remote Host Without scp Support

Problem You backed up your data to a remote host that does not support scp (for example, a Windows PC or server), and you need to retrieve the backup files from the remote host.

Solution Use an SFTP client software program to move the backup files from the remote host to the server, then restore your data from the Local Directory to which you moved the backed-up data.

Perform the following procedure to restore your data from a remote host that does not support scp:

Procedure

Step 1 Access the remote host to where you backed up your data.

Step 2 Open a program that can act as an SFTP program, such as SSH Secure Shell Secure File Transfer Client or similar software. If you are using SSH Secure Shell File Transfer Client, choose **Start > Programs > SSH Secure Shell > Secure File Transfer Client** to connect remotely to the Cisco IPICS server from your PC.

The SSH Secure Shell File Transfer Client window displays. The desktop of your PC displays in the left pane.

Step 3 Click **Quick Connect** to connect to the server.

The Connect to Remote Host window displays.

Step 4 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 5 In the Host field, enter the DNS host name or the IP address for your server. Then, press the **Tab** key.

Step 6 In the User Name field, enter **root**.

Step 7 Click **Connect**.

The Enter Password window displays.

Step 8 Enter the password for the root user and click **OK**.

The SSH Secure Shell File Transfer Client connects to the Cisco IPICS server and displays the contents of the **/root** directory in the right pane of the window.

Step 9 In the left pane of the window, navigate to the folder location on your remote host where you stored the backup files, for example, **C:\My Documents\IDSB2006-11-02_14-04-52**.

Step 10 Choose **Operation > Go to Folder** from the SSH Secure Shell menu bar.

The **Go to Folder** pop-up window displays.

Step 11 In the **Enter Folder Name** field, enter **/idspri/backup**.

The right pane of the window displays the contents of the **/idspri/backup** folder.

Step 12 Drag the backup folder on your PC from the left pane of the window to the right pane to initiate the copy procedure.

A progress window displays while the file copies from your PC to the **/devices** directory. When the copy completes, the backup folder displays in the right pane, for example **IDSB2006-11-02_14-04-52**.

Step 13 Click the **New Terminal Window** icon or choose **Window > New Terminal** from the menu bar to open a terminal window session.

Step 14 Enter the following command to change the ownership of the backup folder and files:

[root]# **chown -R informix:ipics /idspri/backup/IDSB***

Step 15 Enter the following command to enable Cisco IPICS to read from and write to the backup folder and files:

[root]# **chmod -R 550 /idspri/backup/IDSB***

Step 16 Close the SSH Secure Shell terminal window.

Step 17 Close the SSH Secure Shell File Transfer Client.

Step 18 Restore your files from the local directory by following the procedure in the "Performing the Restore Procedure" section on page 9-14. Be sure to specify the **/idspri/backup** directory, as well as the entire path name of the **IDSB***yyyy-mm-dd_hh-mm-ss* directory, when performing the local restore operation.

Unable to Log In To the Administration Console After Restoring Data

If you cannot log in to the Administration Console after you restore your data, note any errors that you receive in your browser and compare the error against the problem descriptions that follow. Then, perform the procedure that is listed in the corresponding solution to attempt to fix your problem.

Problem You performed a restore operation. After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 9-17, you determine that the restore process has completed

successfully. When you attempt to log in to the Cisco IPICS console, you receive a "Cannot find server or DNS Error" error message in the Internet browser, and you cannot access the Administration Console.

Solution It is possible that the Tomcat service was not restarted after the restore operation. To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server using the root user ID.

Step 2 To restart the Tomcat service and the policy engine, enter the following command at the prompt:

[root]# **service ipics restart**

Note Cisco IPICS cancels any active policy engine dial-in or dial-out calls when you enter the service **ipics restart** command.

The Tomcat service and the policy engine stops and restarts.

Step 3 Log in to the Administration Console.

Problem After checking the status of the restore operation as described in the "Checking the Restore Status in the Database Log" section on page 9-17, you determine that the restore process has completed successfully. When you attempt to log in to the Cisco IPICS console, you receive the following pop-up window:

```
You entered an invalid name or password.
Please try again.
If this problem persists, the database may be unavailable. Contact
your system administrator for help.
```

Solution It is possible that the Cisco IPICS database did not restart after the restore operation. To restart the Tomcat service, perform the following procedure:

Procedure

Step 1 Open a terminal window and log in to the server using the root user ID.

Step 2 To check the status of the database, enter the following command at the prompt:

[root]# **onstat -**

If the database is online and running, the command displays the following response.

```
IBM Informix Dynamic Server Version 10.00.UC1 -- On-Line -- Up
00:16:14 -- 124036 Kbytes
```

If the database is not running, the command displays the following response:

```
shared memory not initialized for INFORMIXSERVER 'IPICSDBServer'
```

Step 3 If the database is not running, manually start the Informix database by entering the following command at the prompt:

[root]# **service ipics_db start**

Step 4 Log in to the Administration Console.

Unable to Retrieve a Database Backup from a Remote Host after Reinstalling Cisco IPICS

Problem You reinstalled the Cisco IPICS operating system software server software and attempted to restore your data from a remote host. The restore operation failed.

Solution When you reinstall the Cisco IPICS operating system, the host keys that are used by the scp process are deleted from the Cisco IPICS system. These host keys are used by the remote system for authentication purposes. In this case, the host keys that are used by the remote system to authenticate the Cisco IPICS system no longer match the host keys for the newly-installed Cisco IPICS system.

To configure the remote host so that the new host keys are recognized, perform the following steps:

Procedure

Step 1 Open a terminal window to the remote host by using SSH Secure Shell Client software or similar software.

Step 2 Log in to the remote host by using the same user name that you used for the database backup to the remote host.

Step 3 Open a secure shell terminal to the Cisco IPICS server by entering the following command:

ssh <*ip_address*> | <*dns_name*>

where:

<*ip_address*> or <*dns_name*> represents the IP address or DNS host name of the server.

You should receive a message similar to the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@        WARNING: HOST IDENTIFICATION HAS CHANGED!        @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key in /yoursystem/ssh/known_hosts to get rid of this
message.
Agent forwarding is disabled to avoid attacks by corrupted servers.
X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)?
```

Step 4 Enter **Yes** at the prompt to accept the new public host key for the Cisco IPICS server.

Step 5 Enter **exit** at the prompt to log out of the Cisco IPICS server.

Step 6 Enter **exit** at the prompt to log out of the remote host.

Step 7 Retry the restore operation from the Cisco IPICS Administration Console as described in the "Restoring Data from a Database Backup" section on page 9-12.