Perform Backup and Restore

This section explains the following:

Perform Backup and Restore

You can schedule periodic backups using the Cisco Prime Collaboration Assurance user interface.

Cisco Prime Collaboration Analytics data is backed up on a remote server using SSH. It does not use the Cisco Prime Collaboration Assurance backup repository. You can backup the analytics data only through User Interface, and restore the data through CLI.

Note Linux server is recommended for Cisco Prime Collaboration Analytics backup.

You can also backup Cisco Prime Collaboration Analytics on Windows server. Backup supports in Cygwin UNIX shell. Backup support in Windows server is not available using other SSH tools or Unix Shell.

Related Topics

Monitor Conferences
Troubleshooting Workflow for Video Endpoints
Purge Policies
Concepts

Overview of Backup and Restore

Cisco Prime Collaboration Assurance uses the following purge policy:

- All conference and endpoint statistics data older than one day are purged.
- **For Cisco Prime Collaboration Release 11.5 and later**

  All conference and troubleshooting details older than 14 days are purged every hour.
- **For Cisco Prime Collaboration Release 11.6 and earlier**

  Call quality event history and audio/video phone audit report data older than 30 days are purged.

For Cisco Prime Collaboration Release 12.1 and later

Call quality event history and endpoint related audit report data older than 30 days are purged.

- Cleared alarms and events that are older than 14 days are purged every hour. If an alarm is purged, all associated events are also purged. Active events and alarms are not purged.
- Jobs that are older than 14 days and have a status of completed, failed, or cancelled are purged every hour.

The backup and restore service allows you back up the database, configuration files, and log files to either a remote location or a local disk. Files in following folders are backed up by the backup service:

Type of Data for Assurance Backup
Assurance database
Configuration files

Type of Data for Analytics Backup
Analytics database
Log files
Reports (Scheduled Reports and Custom Reports)
Logos

Schedule Backup using Cisco Prime Collaboration Assurance and Analytics User Interface

For Cisco Prime Collaboration Release 11.1 and earlier

You can schedule and run backup for both Assurance and Analytics from the user interface.

For Cisco Prime Collaboration Release 11.5 and later

You must be logged in as an administrator to perform backup.

To create a new backup job:

Step 1 Choose **System Administration** > **Backup settings**.

Step 2 On the Backup page, click **New**.

Step 3 Enter a name for the backup job.

If backup name is not specified, the **Backup Title** field is defaulted with date stamp.

Step 4 Select the **Backup Category** from the drop-down list.

Step 5 In the **Assurance Connection Settings** pane, enter the following details.

You can use sFTP, FTP, or local connection to create backup.

If you select sFTP or FTP, provide the following details:

- IP address of the server where the backup files need to be saved
- Path to the backup location

Note The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Assurance backup location will be /backup/assurance_backup.
The backup is saved in /user1/backup/assurance_backup.	

- Port (for sFTP only)
- Username
- Password

Click **Test** to test the sFTP or FTP connection using the credentials.

If you select local, specify the location to save the backup files on your local machine.

For a local backup, you can specify the number of backup files to be saved, using the **Backup History** drop-down list. By default, the last two backup files are saved. You can save up to nine backup files.

The Analytics Connection Settings pane is available only if you have enabled Cisco Prime Collaboration Analytics.

For Cisco Prime Collaboration Release 11.5 and later

Cisco Prime Collaboration Analytics is supported on the MSP deployments.

Step 6 In the **Analytics Connection Settings** pane, enter the following details.

You can use only a remote server to backup the Analytics data using SSH.

- IP address of the remote server where the backup files need to be saved
- Path to the backup location. You must provide relative path.

Note The backup is taken in the specified user home directory. For example,

Field	Description
SSH Username	Enter a name for the SSH Username. For example, user1 or provide any desired name.
Path	Enter a name for the path. For example, /backup Then, the Analytics backup location will be /backup/pg_basebackup (followed by timestamp (for example, pg_basebackup_201707201255)).
The backup is saved in /user1/backup.	

The Analytics backup folder will be in the following format: pg_basebackup (followed by the timestamp (for example, pg_basebackup_201707201255)). The backup fails if the user does not exist on the sFTP server.

- SSH Port
- SSH Username
- SSH Password

Click **Test** to test the connection using the credentials.

Step 7 Specify the backup start time and recurrence interval.

The time displayed in the date picker is the client browser time.

Step 8 (Optional) Enter the email IDs to which the backup status notification needs to be sent. Separate the email IDs using comma.

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**E-mail Setup for Alarms & Events**) to receive emails.

For Cisco Prime Collaboration Release 11.5 and later

Configure the SMTP server details in the Cisco Prime Collaboration Assurance server (**Alarm & Report Administration** > **E-mail Setup for Alarms & Events**) to receive emails.

Step 9 Click **Save**.

The scheduled backup job is listed on the **Backup Management** page.

You can click **Run Now** to run the backup immediately.

Troubleshooting

Issue: Cisco Prime Collaboration Assurance backup job status shows failure even after generating the reports. The backup files are generated and stored in a sFTP location when a backup job is scheduled in the Cisco Prime Collaboration Assurance. A non-zero size file is created at the location. The job scheduled in the Cisco Prime Collaboration Assurance is in the failed state every time it is executed.

Expectation: The job must not fail or if it fails there must be reasons for failure.

The Cisco Prime Collaboration Assurance backup job status displays failure in spite of generating reports in sFTP. Hence, while backing up, modify the path of the sFTP server. Use a non-root user location for setting up the sFTP location for reports in the Cisco Prime Collaboration Assurance. The issue is due to the absence of the GPG key in the user folder.

The sFTP location for backup can be any other directory other than the root directory since GPG encryption is not enabled for the root directory.

If you choose the location under the root directory, then you must enable GPG encryption in the root directory.

Check the Backup History

You can check the backup history. Log in to the Cisco Prime Collaboration Assurance server.

Path: **System Administration** > **Backup Settings**

All the backups scheduled or configured are listed on the Backup Settings page. You can check the history from the **Run History** column. Click the hyperlink on each log listed in the column for more information.