Data Collection and Purging

- Control Data Collection Jobs, page 1
- How Data Retention Settings Affect Web GUI Data, page 1
- Performance and System Health Data Retention, page 2
- Alarm, Event, and Syslog Purging, page 3
- Log Purging, page 3
- Report Purging, page 4
- Backup Purging, page 4
- Device Configuration File Purging, page 4
- Software Image File Purging, page 4

Control Data Collection Jobs

All data collection tasks (and data purging tasks) are controlled from the Jobs Dashboard. See Manage Jobs Using the Jobs Dashboard. Data collection jobs are listed under System Jobs .

How Data Retention Settings Affect Web GUI Data

Changes you make on the Data Retention page determine the information that is displayed in the web GUI. You can open the data retention page by choosing **Administration** > **Settings** > **System Settings**, then choosing **General** > **Data Retention**.

For example, if you do not need any historical performance data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retention Period—1 day
- Medium-term Data Retention Period—3 days
- Long-term Data Retention Period—7 days

If you specify these settings, all data displayed in performance reports and on performance dashboards will be for the previous 7 days only. When you generate a performance report, even if you select a reporting period longer than the last 7 days, the report will contain data from the last 7 days only (because that is all of the data you selected to retain).

Similarly, if you view a performance dashboard and select a time frame longer than one week, the dashboard will contain date from the last 7 days only.

Performance and System Health Data Retention

Note Cisco recommends you do not change the retention periods for trend, device health, system health, and performance data because the default settings are optimized to get the most helpful information from interactive graphs.

The following table describes the information shown on the Data Retention page.

Type of Data	Description	Default Retention Settings
Trend	Device-related historical information. Trend data is gathered as a whole and summarized as minimums, maximums, or averages.	Hourly data: 15 Daily data: 90 Weekly data: 54 weeks
Device health	SNMP-polled device data such as device reachability, and utilization for CPU, memory, and interfaces.	Hourly data: 15 Daily data: 90 Weekly data: 54 weeks
Performance	Assurance data such as traffic statistics. • Short-term data is aggregated every 5 minutes. • Medium-term data is aggregated every hour. • Long-term is aggregated daily	Short-term data: 7 Medium-term data: 31 Long-term data: 365 days
Network audit	Audit records for configurations triggered by users, and so on.	90 days
System health	Includes most data shown on the Admin dashboards	Hourly data: 15 Daily data: 90 Weekly data: 54 weeks

For example, these are the retention settings for optical performance data:

- Optical 15-minute performance data (short-term) is saved for 7 days.
- Optical 1-day performance data (medium-term) is saved for 31 days.

Alarm, Event, and Syslog Purging

Note These default purging settings are provided to ensure optimal performance. Use care when adjusting these settings, especially if Cisco EPN Manager is managing a very large network (where increasing these settings may have an adverse impact).

Cisco EPN Manager stores a maximum of 8000000 events and 2000000 syslogs in the database.

To protect system performance, Cisco EPN Manager purges alarms, events, and syslogs according to the settings in the following table. All of these settings are enabled by default. Data is deleted on a daily basis. Alarm tables are checked hourly, and if the alarm table exceeds the 300,000 limit, Cisco EPN Manager deletes the oldest cleared alarms until the alarms table size is within the limit.

Data Type	Deleted after:	Default Setting
Alarms—Cleared security alarms	30 days	Enabled
Alarms—Cleared non-security alarms	7 days	Enabled
Events	60 days	Enabled
Syslogs	30 days	Enabled
Alarms	30 days	Disabled

To change the settings, choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events** and modify the settings in the Alarm and Event Cleanup Options area.

Log Purging

You can adjust the purging settings for logs by choosing **Administration** > **Settings** > **Logging** . Logs are saved until the reach the maximum size. At that point, a number is appended to the log file and a new log is started. When the number of logs exceeds the maximum, the oldest log is deleted.

The following table lists the default purging values for General and SNMP logs.

Log Type	Size of Logs	Number of Logs	To change the setting, see:
General	10 MB	10	Adjust General Log File Settings and Default Sizes
SNMP	10 MB	5	View and Manage General System Logs

Report Purging

By default, reports are stored in a repository named /localdisk/ftp/reports and are deleted after 31 days from that directory. Reports filters that you set from the filters page are saved in the database and are not purged.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Reports**.

Step 2 If required, adjust the location for the reports repository on the server. The repository must reside under the FTP root partition.

Step 3 If you want to change the default purging age, enter a new value in the **File Retain Period** field.

Step 4 Click **Save**.

Backup Purging

By default, 2 backups are saved for backups in local repositories. If you are using remote repositories, there is no automatic backup purging mechanism; you must manually delete old backups. See Change the Number of Automatic Application Backups That Are Saved.

Device Configuration File Purging

For each device, 5 configuration files are saved in the configuration archive. Any file that is older than 30 days is purged. Device configuration files cannot be manually deleted. For more information on device configuration files, see Manage Device Configuration Files.

Software Image File Purging

Device software image files are not automatically purged from the database. They must be manually removed using the GUI client. For more information, see Delete Software Image Files from the Image Repository.