Data Collection and Background Tasks

Check Data Purging Settings

Performance, Health, and Audit Data Purging

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 different types of data that are listed 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 days Daily data: 90 days Weekly data: 54 weeks
Device health	SNMP-polled device data such as device reachability, QoS, and utilization for CPU, memory, and interfaces.	Hourly data: 15 days Daily data: 90 days Weekly data: 54 weeks

Type of Data	Description	Default Retention Settings
Performance	Assurance data such as traffic statistic. • Short-term data is aggregated every 5 minutes. • Medium-term data is aggregated every hour. • Long-term is aggregated daily	Short-term data: 7 days Medium-term data: 31 days Long-term data: 378 days
Network audit	Network audit logs	90 days
System health	System audit logs	Hourly data: 15 days Daily data: 90 days 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).

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.

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

The following setting is disabled by default.

Data Type	Deleted after:	Default Setting:
Alarms (all)	30 days	Disabled

To change the settings, choose **Administration > Settings > System Settings,** then choose **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 > System Settings**. then selecting **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 select **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 Adjust Backup Settings.

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 Repository.

LIMITED ORDERABILITY RELEASE

Adjust When Server Data Is Collected

The Background Tasks page lists a variety of processes that run in the background of Cisco EPN Manager.

Note Data collected by enabled monitoring policies are controlled as jobs. To check their status, select Administration > Jobs, or check the status as described in Check the Status of Past Data Collections.

To view the background tasks, choose **Administration > Background Tasks** and click the task hyperlink for details. Depending on the task type, you can:

- Disable or enable the background task
- Change the polling interval

The following table describes the various data collection tasks in Cisco EPN Manager.

Table 22-1 Data Collection Tasks

Type	Task Name	Task Status	Runs every:	Description
Data Collection	Switch Inventory	Enabled	24 hours	Discovers and collects inventory information for all devices
Other	Appliance Status	Enabled	5 minutes	Checks the status of the virtual machines
	Data Cleanup	Enabled	24 hours	Purges old data from the system
	License Status	Enabled	4 hours	Checks the status of all licenses (Right To Manage, time-based licenses, and so forth)
	OSS Server Status	Enabled	5 minutes	Checks the status of the API
	EPN Server Backup	Enabled	24 hours	Backs up the Cisco EPN Manager data
	Switch Operational Status	Enabled	5 minutes	Checks switch status and triggers full status check if needed
		Enabled	60 minutes	Checks the full switch status