Data Collection and Purging

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 .

About System Jobs

The following table describes the background data collection jobs Cisco EPN Manager performs.

Table 1: Inventory Data Collection Jobs

Task Name	Default Schedule	Description	Editable options
Infrastructure jobs			
Data Cleanup	2 hours	This job schedules daily data file cleanup.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Device Config Backup-External	15 minutes	This Job will Export all device configs (Text-Files in a Zip) to a predefined external repository. You can configure or create the repository using CLI commands and the supported repositories are FTP, SSH FTP (SFTP) and Network File System (NFS).	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job. Click the edit icon, and check the **Export only Latest Configuration** check box, to transfer only the latest configuration. You can edit the job properties based on the user permission set in Role Based Access Control (RBAC).
Index search Entities	3 hours	This Job schedules the Index Search Entities.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
On Demand Reports Cleanup	6 hours	This job schedules reports cleanup when required.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Server Backup	1 day	This job schedules automatic Cisco EPN Manager server backups. The backups created are application backups.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Smart License Compliance Status	Disabled	This job runs for Smart License for the default schedule.	Non Editable.
Inventory and Discovery Jobs			
Switch Inventory	1 day	This job collects inventory for discovered devices which are reachable periodically as per given schedule.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
failedFeatureSync	30 minutes	This job collects inventory for the only failed features for devices in CWW and do a full sync for devices CF periodically, this job is suspended by default. Customers can enable it based on their choice.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Status Jobs			

Task Name	Default Schedule	Description	Editable options
Autonomous AP Operational Status	5 minutes	This job schedules status polling of autonomous wireless access points.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Switch Operational Status	5 minutes	This job checks for the node reachability.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Third Party Access Point Operational Status	3 hours	This job schedules operational status polling of third party APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Third Party Controller Operational Status	3 hours	This job schedules operational status polling of third party Controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless AP Discovery	5 minutes	This job schedules Wireless AP discovery.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

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.

When you create the monitoring policy for interfaces, you can define the polling interval for every 15 minutes or every 5 minutes or every 1 minute. According to the selected polling interval, the device data is polled and

stored in Oracle Data base. The data is aggregated every 1 hour into the AHxxx table; once a day into the ADxxx table irrespective of the polling interval is set to1/5/15 minutes.

In the Interface Health Policy tab, if the frequency is set at 5 mins, you can view 12 samples for each hour. Every hour the data moves to the aggregated table and an average or mean interface statistics is calculated , and there will be one entry in the hourly aggregated table. The aggregation is the same for all the policies no matter what the polling interval is.

You can view data retention details and the age of the data storage, the event time in milliseconds and for each data base the entity ID and the event time.View the performance data and aggregate data in the Performance Dashlet, > Interfaces > Traffic Utilization tab.

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 Data Retain Periods	Device-related historical information. Trend data is gathered as a whole and summarized as minimums, maximums, or averages.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)
Device Health Data Retain Periods	SNMP-polled device data such as device reachability, and utilization for CPU, memory, and interfaces.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)
Performance Data Retain Periods	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 retain period: 7 (days) Medium term data retain period: 31 (days) Long term data retain period: 378 (days)
Network Audit Data Retain Period	Audit records for configurations triggered by users, and so on.	Audit data retain period: 90 (days)
System Health Data Retain Periods	Includes most data shown on the Admin dashboards	Hourly data retain period: 1 (days) Daily data retain period: 7 (days) Weekly data retain period: 54 (weeks)

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

- Optical 30 seconds performance data (short-term) is saved for 1 hour.
- Optical 15-minute performance data (short-term) is saved for 7 days.
- Optical 1-day performance data (medium-term) is saved for 30 days.

Specifying Data Retention By Database Table

Administrators can use the "Other Data Retention Criteria" section of the Data Retention page to configure retention periods for specific Cisco EPN Manager database tables. You specify the retention period using the following attributes:

- **Age (in hours)** : Specifies the maximum data retention period in hours for all records in the database.
- **Max Records** : Specifies the maximum number of records to retain in a particular database table. A Max Records value of NA means that the only retention criteria considered is the Age attribute.

The section is categorized into multiple subsections. Each subsection list each database table name, along with the current Age and Max Records used to determine whether an individual record in the table will be retained or discarded. The page also lists the table Age Attribute used to compute the age of the data in the table.

Cisco strongly recommends that you consult with Cisco Technical Assistance Center before changing the values for any of the tables in this section. Doing so without help may affect system performance negatively.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **General** > **Data Retention**.

Step 2 Expand the **Other Data Retention Criteria** section.

Step 3 Expand the database table subsection for which you want to specify Age and Max Records values.

Step 4 Click on the database table listing and enter the new values as needed.

Step 5 Click **Save**.

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.