Managing Data Collection and Retention

One of the roles of an administrator is to manage Prime Infrastructure's network data collection and retention so that it:

- Scales to fit the real needs of the system's users.
- Minimizes the burden on monitored devices, applications, and network bandwidth.
- Survives hardware failures.

The following topics explain how to achieve these goals and perform other data management tasks.

Specifying Data Retention Periods

You can configure retention periods for trend data, device health data, and system health data on an hourly, daily, and weekly basis. You can configure retention periods for performance data on a short, medium, and long term basis.

To set retention periods for aggregated data used in timed calculations and network audit calculations:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Data Retention**. The Data Retention page appears.

Step 3 Modify the values as required. See Table 6-1 for the default values.

Note For the best interactive graph data views, change the settings to default value.

Step 4 Click **Save**.

Prime Infrastructure Historical Data

There are two types of historical data in Prime Infrastructure, including the following:

- Aggregated historical data—Numeric data that can be gathered as a whole and aggregated to minimum, maximum, or average. Client count is one example of aggregated historical data.

  Use the **Administration > System Settings > Data Retention** page to define the aggregated data retention period. Aggregation types include hourly, daily, and weekly.

  The retention period for these aggregation types are defined as Default, Minimum, and Maximum (see Table 6-1).

Table 6-1 Data Retention Periods

Trend Data[1] Retain Periods			
Period	**Default**	**Minimum**	**Maximum**
Hourly	15	1	31
Daily	90	7	365
Weekly	54	2	108
Device Health Data[2] Retain Periods			
Hourly	15	1	31
Daily	90	7	365
Weekly	54	2	108
Performance Data[3] Retain Periods			
Short Term Data	7	1	31
Medium Term Data	31	7	365
Long Term Data	378	2	756

Table 6-1 Data Retention Periods (continued)

Network Audit Data Retain Period			
Audit Data Retain Period	90	7	365
System Health Data Retain Periods			
Hourly Data Retain Period	1	1	31
Daily Data Retain Period	7	7	365
Weekly Data Retain Period	54	7	365

1. Trend data includes wireless-related historical information such as client history, AP history, AP utilization, and client statistics.
2. Device Health data includes SNMP polled data for wired and wireless devices such as device availability, and CPU, memory, and interface utilization, and QoS.
3. Performance data includes Assurance data such a traffic statistics, application metrics, and voice metrics.

- Non-aggregated historical data—Numeric data that cannot be gathered as a whole (or aggregated). Client association history is one example of non-aggregated historical data.

  You can define a non-aggregated retention period in each data collection task and other settings.

  For example, you define the retention period for client association history in **Administration > System Settings > Client**. By default, the retention period is 31 days or 1 million records. This retention period can be increased to 365 days.

Performance Data Aggregation

The Performance Data is aggregated as follows:

- Short-term data is aggregated every 5 minutes.
- Medium-term data is aggregated every hour.
- Long-term is aggregated daily.

Enabling Data Deduplication

Data Deduplication allows you to identify authoritative sources for each of the following classes of application data:

- Application Response Time (for TCP applications)
- Voice/Video (for RTP applications)

Whenever Prime Infrastructure receives duplicate data about the same network elements and protocols from two or more data sources, it resolves all such conflicts in the authoritative source's favor.

The Data Deduplication page allows you to specify a data source at a specific site. For example, if you have a Network Analysis Module (NAM) at a branch office as well as NetFlow data that is sent from the same branch, you can specify which data source Prime Infrastructure uses.

To enable data deduplication:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Data Deduplication**. The Data Deduplication page appears.

Step 3 Select the **Enable Data Deduplication** check box to remove the duplicated information from Prime Infrastructure, then click **Apply**.

Specifying Where and for How Long to Save Reports

To indicate where the scheduled reports reside and for how many days:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Report**. The Report page appears.

Step 3 Enter the path for saving report data files on a local PC. You can edit the existing default path.

Step 4 Specify the number of days to retain reports.

Step 5 Click **Save**.

Controlling Report Storage and Cleanup

All scheduled reports are stored in the Scheduled Reports Repository. You will want to ensure that scheduled reports are retained in the report repository for reasonable lengths of time only, and deleted on a regular basis. The default retention scheme is to retain generated reports for a maximum of 31 days.

To customize the retention period:

Step 1 Choose **Administration > System Settings.**

Step 2 From the left sidebar menu, choose **Report**. The Report page appears.

Step 3 In **Repository Path**, specify the report repository path on the Prime Infrastructure server.

Step 4 In **File Retain Period**, specify the maximum number of days reports should be retained.

Step 5 Click **Save**.

Specifying Inventory Collection After Receiving Events

The Inventory page allows you to specify if Prime Infrastructure must collect inventory when a syslog event is received for a device.

To configure the inventory settings:

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Inventory**. The Inventory page appears.

Step 3 Select the **Enable event based inventory collection** check box to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device.

Step 4 Select the **Enable Syslog and Traps on device** check box to allow Prime Infrastructure to enable syslog and trap notifications on newly added devices.

Step 5 Click **Save**.

Device Configuration Settings

Backing up and Rolling Back Configurations

You can back up and roll back the running configuration from the **Administration > System Settings > Configuration** page.

Step 1 Choose **Administration > System Settings**.

Step 2 From the left sidebar menu, choose **Configuration**.

Step 3 Enter the required information.

Step 4 Click **Save**.

Specifying When to Archive Configurations

Configuration archive/rollback is only supported for running-config on devices with WLC software. It is not supported for startup-config.

The configuration changes (such as turning on/off options) that you perform in the Administration > System Settings > Configuration page have no relevance to configuration archive operations. The configurations that you perform in this page are related to template deployment. For example, Backup running Configuration is to archive configuration before any template is deployed.

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives notification of a configuration change event

To change when Prime Infrastructure archives configurations:

Step 1 Choose **Administration > System Settings > Configuration Archive**.

Step 2 Change the necessary settings.

Step 3 To have Prime Infrastructure ignore commands for a particular device type, click the **Advanced** tab, choose the device type, and enter the commands to be ignored.

If the device you specify has a change in its configuration and Prime Infrastructure detects that the change is in one of the commands in the exclude list, Prime Infrastructure does not create an archived version of the configuration with this change.

Step 4 Click **Save**.

Controlling Background Data Collection Tasks

Prime Infrastructure performs scheduled data collection tasks on the background on a regular basis. You can enable or disable these collection tasks, change the interval at which each task is performed, or change the retention period for the data (raw or aggregated) collected during each task.

Disabling or limiting these background data collection tasks can have a direct impact on how you use Prime Infrastructure, especially for reporting. To help you consider these impacts, take note of the reports this data is used in. These reports are listed in the Collection Set Details for each task.

To create a background data collection task:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Under **Data Collection Tasks**, in the **Task** column of the table, click the name of the task that you want to create.

Step 3 Enter the required information and click **Save**.

To enable or disable background data collection tasks in bulk:

Step 1 Choose **Administration > Background Tasks**.

Step 2 Under **Data Collection Tasks**, select the check box next to each task you want to enable or disable.

Step 3 Choose **Go**, then choose to either enable or disable tasks.

Understanding What Data Is Collected and When

The following table describes the various data collection tasks in Prime Infrastructure.

Table 6-2 Data Collection Tasks

Task Name	Task Status	Default Schedule	Description
AP Image Pre-Download Status	Disabled	15 minutes	Allows you to see the Image Predownload status of the associated APs in the controllers. To see the status of the access points, the Pre-download software to APs check box should be selected while downloading software to the controller.
Autonomous AP CPU and Memory Utilization	Enabled	15 minutes	Collects information about memory and CPU utilization of autonomous APs.
Autonomous AP Inventory	Enabled	180 minutes	Collects the inventory information for autonomous APs.
Autonomous AP Radio Performance	Enabled	15 minutes	Collects information about radio performance information as well as radio up or down status for autonomous APs.
Autonomous AP Tx Power and Channel Utilization	Enabled	30 minutes	Collects information about radio performance of autonomous APs.
CCX Client Statistics	Disabled	60 minutes	Collects the Dot11 and security statistics for CCX Version 5 and Version 6 clients.
CleanAir Air Quality	Enabled	15 minutes	Collects information about CleanAir air quality.
Client Statistics	Enabled	15 minutes	Retrieves the statistical information for the autonomous and lightweight clients.
Controller Performance	Enabled	30 minutes	Collects performance information for controllers.
Guest Sessions	Enabled	15 minutes	Collects information about the guest sessions.
Interferers	Enabled	15 minutes	Collects information about the interferers.
Media Stream Clients	Enabled	15 minutes	Collects information about media stream for clients.
Mesh link Performance	Enabled	10 minutes	Collects information about the performance of Mesh links.
Mesh Link Status	Enabled	5 minutes	Collects status of the Mesh links.
Mobility Service Performance	Enabled	15 minutes	Collects information about the performance of mobility service engines.
Radio Performance	Enabled	15 minutes	Collects statistics from wireless radios.
Radio Voice Performance	Enabled	15 minutes	Collects voice statistics from wireless radios.
Rogue AP	Enabled	120 minutes	Collects information about the rogue access points.
Switch CPU and Memory Poll	Enabled	30 minutes	Collects information about switch CPU and memory poll.
Switch Inventory	Enabled	Daily at midnight	Collects inventory information for switches.
Traffic Stream Metrics	Enabled	8 minutes	Retrieves traffic stream metrics for the clients.
Unmanaged APs	Enabled	15 minutes	Collects poll information for unmanaged access points.

Table 6-2 Data Collection Tasks (continued)

Task Name	Task Status	Default Schedule	Description
Wireless Controller Inventory	Disabled	Daily at midnight	Collects inventory information for wireless controllers.
Wireless Controller Performance	Enabled	30 minutes	Collects performance statistics for wireless controllers.

Controlling Prime Infrastructure Background Tasks

The following table describes the background tasks Prime Infrastructure performs. You can manage how and when they are performed by selecting **Administration > System Settings > Background Tasks**, then selecting the hypertext link for that task in the Other Background Tasks area of the page.

Table 6-3 Other Background Tasks

Task Name	Default Schedule	Description	Editable Options
Appliance Status	5 minutes	Lets you view appliance polling details. This task populates the appliance polling details from the **Administration > Appliance > Appliance Status** page. In addition, this background task populates information such as the performance and fault checking capabilities of the appliance.	Default—Enabled. Interval—Valid interval is from 1 to10080.
Autonomous AP Operational Status	5 minutes	Lets you view the autonomous AP operational status polling.	Default: Enabled Interval—Valid interval is from 1 to10080.
Autonomous Client Status	5 minutes	Lets you discover the autonomous AP client from the network.	Default—Enabled.
Configuration Sync	Daily at 4 am.	Lets you view the configuration synchronization.	Enable—Click this check box to enable configuration synchronization. Default: Enabled. Enable—Click this check box to enable Network Audit. Default: Enabled. Enable—Click this check box to enable Security Index calculation. Default: Enabled. Enable—Click this check box to enable RRM audit. Default: Enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Controller Configuration Backup	Daily at 10 pm	Lets you view controller configuration backup activities.	Enable—Click this check box to enable controller configuration backup. Default: Disabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration synchronization to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM. TFTP Server—Select the IP address of the server to which you want to back up the controller configuration.
Controller Operational Status	5 minutes	Lets you schedule and view controller operational status.	Enable—Click this check box to enable Controller Configuration Backup. Default: Enabled. Interval—Enter the interval, in days, that you want the configuration synchronization to happen. The valid range is 1 to 360 days.
Data Cleanup	Daily at 2 am.	Lets you schedule a data cleanup.	Time of Day—Enter the time of the day that you want the data cleanup to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM. Default: Enabled.
Device Data Collector	30 minutes	Lets you schedule data collection based on specified command-line interface (CLI) commands at a configured time interval.	Enabled—Click this check box to enable data collection for a specified controller. The default is Disabled. Controller IP address—The IP address of the Controller to collect data from. CLI Commands—Enter the CLI commands, separated by commas, that you want to run on the specified controller. Clean Start—Click this check box to enable a clean start before data collection. Repeat—Enter the number of times that you want the data collection to happen. Interval—Enter the interval, in days, that you want the data collection to happen. The valid range is 1 to 360 days.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Guest Accounts Sync	Daily at 1 am.	Schedules guest account polling and synchronization.	Enable—Click this check box to enable guest account synchronization. The default is Enabled. Interval—Enter the interval, in days, that you want the guest account synchronization to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the guest account synchronization to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM.
Identity Services Engine Status	15 minutes	Schedules the Identity Services Engine polling.	Enable—Click this check box to enable Identity Services Engine polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Identity Services Engine polling to happen. The valid range is 1 to 360 days.
License Status	4 hours.	Schedules license status polling.	Enable—Click this check box to enable license status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the license status polling to happen. The valid range is 1 to 360 days.
Lightweight AP Operational Status	5 minutes.	Lets you view Lightweight AP operational status polling.	Enable—Click this check box to enable Lightweight AP Operational Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight AP Operational Status polling to happen. The valid range is 1 to 360 days.
Lightweight Client Status	5 minutes.	Lets you discover Lightweight AP clients from the network.	Enable—Click this check box to enable Lightweight Client Status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the Lightweight Client Status polling to happen. The valid range is 1 to 360 days.
Mobility Service Backup	Every 7 days at 1 am.	Schedules mobility services backup polling.	Enable—Click this check box to enable mobility service backup. The default is disabled. Interval—Enter the interval, in days, that you want the mobility services back up to happen. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the mobility services back up to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Mobility Service Status	5 minutes.	This task is used to schedule mobility services status polling.	Enable—Click this check box to enable mobility services status polling. The default is Enabled. Interval—Enter the interval, in days, that you want the mobility services status polling to happen. The valid range is 1 to 360 days.
Mobility Service Synchronization	60 minutes.	This task is used to schedule mobility services synchronization.	Out of Sync Alerts—Click this check box if you want to enable out of sync alerts. Smart Synchronization—Click this check box if you want to enable smart synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the mobility services synchronization to happen. The valid range is 1 to 10080 minutes.
Mobility Status Task	5 minutes	This task is used to view the status of mobility services engine(s).	Enable—Click this check box to enable mobility status polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the mobility status polling to happen. The valid range is 1 to 10080 minutes.
Prime Infrastructure Server Backup	Every 7 days at 1 AM (01:00)	This task is used to schedule Prime Infrastructure server backup.	Enabled—Click this check box to enable automatic Prime Infrastructure server backup. The default is Enabled. Backup Repository—The location of the default backup repository where automatic backups are stored. The default is defaultRepo. Max UI backups to keep—The maximum number of automatic backups to keep (applied only if they are stored in the default local repository). Interval—Enter the interval, in days, at which you want automatic Prime Infrastructure server backups to be taken. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want Prime Infrastructure server back up to be taken. Use 24-hour format (for example, 13:49).
OSS Server Status	5 minutes.	This task is used to schedule OSS server status polling.	Enable—Click this check box to enable OSS Server polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the OSS server polling to happen. The valid range is 1 to 10080 minutes.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Redundancy Status	60 minutes	This task is used to view the redundancy status for primary and secondary controllers.	Enabled—Click this check box to enable Redundancy status polling. The default is Disabled. Interval—Enter the interval, in minutes, that you want the Redundancy status polling to happen.
Switch NMSP and Location Status	4 hours	This task is used to schedule the Switch Network Mobility Services Protocol (NMSP) and Civic Location Polling.	Enable—Click this check box to enable Switch NMSP and Civic Location polling. The default is Enabled. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes.
Switch Operational Status	5 minutes. Full poll is 15 minutes.	This task is used to schedule switch operational status polling.	Enable—Click this check box to enable Switch NMSP and Civic Location polling. Interval—Enter the interval, in minutes, that you want the Switch NMSP and Civic Location Polling to happen. The valid range is 1 to 10080 minutes. Full operational status interval—Enter the interval, in minutes. The valid range is 1 to 1440 minutes.
Third party Access Point Operational Status	3 hours	This task is used to schedule the operational status polling of third party APs.	Enabled—Click this check box to enable third party AP operational polling. Interval—Enter the interval, in hours, that you want the third party AP operational status polling to happen. The valid range is 3 to 4 hours.
Third party Controller Operational Status	3 hours	This task is used to schedule the reachability status polling of third party controllers.	Enabled—Click this check box to enable the reachability status polling of third party controllers. Interval—Enter the interval, in hours, that you want the third party controller reachability status polling to happen. The valid range is 3 to 4 hours.

Table 6-3 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
wIPS Alarm Sync	120 minutes.	This task is used to schedule wIPS alarm synchronization.	Enable—Click this check box to enable wIPS alarm synchronization. The default is Enabled. Interval—Enter the interval, in minutes, that you want the wIPS alarm synchronization to happen. The valid range is 1 to 10080 minutes.
Wired Client Status	2 hours.	This task is used to schedule wired client status polling.	Enable—Click this check box to enable wired client status polling. The default is Enabled. Interval—Enter the interval, in hours, that you want the wired client status polling to happen. The valid range is 1 to 8640 hours. Major Polling—Specify two time periods that you want the major pollings to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM.

Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.x on the Windows NT, Solaris and Linux platforms. The following LMS data can be imported into Prime Infrastructure using CAR CLI:

- Device Credential and Repository (DCR) Devices
- Static Groups
- Dynamic Groups
- Software Image Management Repository Images
- User Defined Templates (Netconfig)
- LMS Local Users
- MIBs

Only the Dynamic Groups containing the rule with the following attributes can be imported from LMS.

- PI attribute Name—LMS attribute name
- Contact—System.Contact
- Description—System.Description
- Location— System.Location
- Management_Address—Device.ManagementIpAddress
- Name—System.Name
- Product_Family—Device.Category
- Product_Series—Device.Series
- Product_Type—Device.Model
- Software_Type—System.OStype
- Software_Version—Image.Version

To migrate LMS data to Prime Infrastructure:

Step 1 Identify the FTP server where LMS backup data is stored, then log in to the Prime Infrastructure server as an admin user.

Step 2 Configure the backup location in the Admin Console by entering the following commands:

```
admin# config terminal
admin(config)# repository carsapps
admin(config-Repository)# url
```

(for example, **ftp://10.77.213.137/opt/lms** or **sftp://10.77.213.137/opt/lms** or **fdisk:foldername**)

```
admin(config-Repository)# user root password plain xxxxxxx
admin(config-Repository)# end
```

Step 3 Import the LMS backup into Prime Infrastructure using the following command:

```
admin# lms migrate repository carsapps
```

Step 4 Log back in to the Prime Infrastructure user interface.

The following table lists the locations of the imported LMS data:

LMS Data	Location in Prime Infrastructure
DCR Devices	Operate > Device Work Center
Static Group	Operate > Device Work Center > User Defined Group
Dynamic Group	Operate > Device Work Center > User Defined Group
Software Image Management Repository Images	Operate > Device work Center > Software Image Management
User Defined Templates (Netconfig)	Design > Feature Design > OOTB Templates
LMS Local Users	Administration > Users, Roles & AAA > Users
MIBs	Design > Custom SNMP Templates