Managing Data Collection and Retention

One of the roles of an administrator is to manage Cisco 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.

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

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

Step 3 On the Data Retention page, modify the values as required.

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

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 summarized as minimums, maximums, or averages. 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.

  Types of aggregated historical data include:

  - Trend: This includes wireless-related historical information such as client history, AP history, AP utilization, and client statistics.
  - Device health: This includes SNMP polled data for wired and wireless devices, such as device availability, and CPU, memory, and interface utilization, and QoS.
  - Performance: This includes Assurance data such a traffic statistics, application metrics, and voice metrics
  - Network audit records
  - System health records

- 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.

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.

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**.

Controlling Report Storage and Retention

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.

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.

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**.

Controlling Configuration Deployment Behavior

Administrators can choose to have device configurations backed up or rolled back whenever Prime Infrastructure users deploy new device configuration templates. They can also control how Cisco WLC configurations are archived.

- Archiving Device Configurations Before Template Deployment
- Rolling Back Device Configurations on Template Deployment Failure
- Specifying When and How to Archive WLC Configurations

Archiving Device Configurations Before Template Deployment

With **Backup Device Configuration** enabled, Prime Infrastructure automatically backs up all device running and startup configurations before deploying new configuration templates.

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

Step 2 Select the **Backup Device Configuration** check box.

Step 3 Click **Save**.

Rolling Back Device Configurations on Template Deployment Failure

With **Rollback Configuration** enabled, Prime Infrastructure automatically rolls back each device to its last archived running and startup configurations when any attempt to deploy a new configuration template to the device has failed.

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

Step 2 Select the **Rollback Configuration** check box.

Step 3 Click **Save**.

Specifying When and How to Archive WLC Configurations

By default, Prime Infrastructure keeps a backup archive of running configurations for each device running Cisco Wireless LAN Controller (WLC) software whenever it:

- Collects initial out-of-box inventory for these devices
- Receives notification of a configuration change event for these devices

Configuration archiving is supported for devices running Cisco WLC software only. Only running configurations are archived (startup configurations are excluded).

You can change many of the basic parameters controlling Cisco WLC configuration archiving, including:

- The maximum timeout on all Cisco WLC configuration operations (fetch, archive or rollback).
- The maximum time to to wait before updating the Cisco WLC configuration archive summary information.
- Whether or not to archive configurations at initial inventory collection, after each inventory synchronization, and on receipt of configuration change events.
- Whether or not to mask security information when exporting archived configurations to files.
- The maximum number of archived configurations for each device and the maximum number of days to retain them.
- The maximum number of thread pools to devote to the archive operation. Increasing the default can be helpful with Prime Infrastructure performance during archiving of changes involving more than 1,000 devices.

You can also tell Prime Infrastructure to ignore for archive purposes any change that involves specified commands on devices of a given family, type, or model. This is useful when you want to ignore insignificant or routine changes in a few parameters on one or many devices.

Step 1 In **Lifecycle** view: Choose **Administration > System Settings > Configuration Archive**.

Step 2 On the **Basic** tab, change the basic archive parameters as needed.

Step 3 To specify devices and configuration commands to exclude from archived configurations:

a. Click the **Advanced** tab.

b. In the **Product Family** list, choose the device(s) for which you want to specify configuration commands to exclude.

   Use the List/Tree View dropdown, or click the > icons to drill down to individual product types and models for which you want to specify exclude commands.

c. In the **Command Exclude List,** enter (separated by commas) the configuration commands you want to exclude for the currently selected device family, type, or model.

   If the device(s) you select has configuration changes and Prime Infrastructure detects that the change is one of the specified commands in the Exclude List, Prime Infrastructure will not create an archived version of the configuration with this change.

d. Click **Save**.

e. To remove a specified set of command exclusions for a device family, type or model, select the device(s) in the Product Family list and click **Reset**.

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, follow these steps:

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

Step 2 In the **Data Collection Tasks** area, 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, follow these steps:

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

Step 2 In the **Data Collection Tasks** area, 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 6-1 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 6-1 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 choosing **Administration > System Settings > Background Tasks**, then clicking the hypertext link for that task in the **Other Background Tasks** area of the page.

Table 6-2 Other Background Tasks

Task Name	Default Schedule	Description	Editable Options
Appliance Status	5 minutes	Lets you schedule appliance polling. 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.	Enable—Select this check box to enable appliance status polling. Interval—Enter the interval, in minutes, between polls. The valid range is 1 to 10800 minutes.
Autonomous AP Operational Status	5 minutes	Lets you schedule status polling of autonomous wireless access points.	Enable—Select this check box to enable status polling of autonomous APs. Interval—Valid interval is from 1 to10080.
Autonomous Client Status	5 minutes	Lets you schedule status polling of autonomous AP clients.	Enable—Select this check box to enable autonomous client status polling. Interval—Enter the interval, in minutes, between polls. The valid range is 1 to 10800 minutes.

Table 6-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Wireless Configuration Audit	Daily at 4 am.	This task performs an audit. It verifies the config for mismatches but does not take actions on it.	Enable—Select this check box to enable configuration synchronization. Enable—Select this check box to enable Network Audit. Enable—Select this check box to enable Security Index calculation. Enable—Select this check box to enable RRM audit. Interval—Enter the interval, in days, between each configuration synchronization. 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.
Controller Configuration Backup	Daily at 10 pm	Lets you view controller configuration backup activities.	Enable—Select this check box to enable controller configuration backup. Interval—Enter the interval, in days, between controller configuration backups. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want the configuration backup to happen. The valid format is hh:mm AM|PM. For example, 12:49 AM. TFTP Server—If selected, also choose in the dropdown the TFTP server to which you want to back up the controller configurations. FTP Server—If selected, enter the user name, password, and port address for the FTP server to which you want to back up the controller configurations.
Controller Operational Status	5 minutes	Lets you schedule controller operational status polling.	Enable—Select this check box to enable controller configuration status polling. Interval—Enter the interval, in minutes, between controller status polls. The valid range is 1 to 10800 minutes.
Data Cleanup	Daily at 2 am.	Lets you schedule daily data file 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.

Table 6-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Device Data Collector	30 minutes	Lets you schedule data collection based on specified command-line interface (CLI) commands at a configured time interval.	Enabled—Select this check box to enable data collection for a specified controller. Controller IP address—The IP address of the Controller to collect device data from. CLI Commands—Enter the CLI commands, separated by commas, that you want to run on the specified device. Clean Start—Select this check box to enable a clean start before data collection. Repeat—Enter the number of times that you want the data collection to be repeated. Interval—Enter the interval, in days, between each device data collection. The valid range is 1 to 360 days.
Guest Accounts Sync	Daily at 1 am.	Lets you schedule guest account polling and synchronization.	Enable—Select this check box to enable guest account synchronization. Interval—Enter the interval, in days, between each guest account synchronization. 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	Lets you schedule the Identity Services Engine polling.	Enable—Select this check box to enable Identity Services Engine polling. Interval—Enter the interval, in days, between each Identity Services Engine poll. The valid range is 1 to 360 days.
License Status	4 hours.	Lets you schedule license status polling.	Enable—Select this check box to enable license status polling. Interval—Enter the interval, in days, between each license status poll. The valid range is 1 to 360 days.
Lightweight AP Operational Status	5 minutes.	Lets you schedule Lightweight AP operational status polling.	Enable—Select this check box to enable Lightweight AP Operational Status polling. Interval—Enter the interval, in days, between each Lightweight AP Operational Status poll. The valid range is 1 to 360 days.

Table 6-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Lightweight Client Status	5 minutes.	Lets you discover Lightweight AP clients from the network.	Enable—Select this check box to enable Lightweight Client Status polling. Interval—Enter the interval, in days, between each Lightweight Client Status poll. The valid range is 1 to 360 days.
Mobility Service Backup	Every 7 days at 1 am.	Lets you schedule automatic mobility services backups.	Enable—Select this check box to enable automatic mobility service backups. Max UI backups to keep—Enter the maximum number of automatic mobility services backups to keep. Interval—Enter the interval, in days, between each mobility services backup. The valid range is 1 to 360 days. Time of Day—Enter the time of day that you want each mobility services backup to be taken. The valid format is hh:mm AM|PM. For example, 12:49 AM.
Mobility Service Status	5 minutes.	Lets you schedule mobility services status polling.	Enable—Select this check box to enable mobility services status polling. Interval—Enter the interval, in days, between each mobility services status poll. The valid range is 1 to 360 days.
Mobility Service Synchronization	60 minutes.	Lets you schedule mobility services synchronization.	Out of Sync Alerts—Select this check box to enable out-of-sync alerts. Smart Synchronization—Select this check box to enable smart synchronization. Interval—Enter the interval, in minutes, between each mobility services synchronization. The valid range is 1 to 10080 minutes.
Mobility Status Task	5 minutes	Lets you schedule status polling of mobility services engines.	Enable—Select this check box to enable mobility status polling. Interval—Enter the interval, in minutes, between each mobility status poll. The valid range is 1 to 10080 minutes.

Table 6-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Prime Infrastructure Server Backup	Every 7 days at 1 AM (01:00)	Lets you schedule automatic Prime Infrastructure server backups. The backups created are application backups.	Enabled—Select this check box to enable automatic Prime Infrastructure server backup. Backup Repository—Enter the name of the local or remote backup repository where automatic backups are stored. Max UI backups to keep—Enter the maximum number of automatic backups to keep (affects local repositories only). Interval—Enter the interval, in days, between each automatic Prime Infrastructure backup. The valid range is 1 to 360 days. Time of Day—Enter the time of the day that you want Prime Infrastructure server backups to be taken. Use 24-hour format (for example, 13:49).
OSS Server Status	5 minutes.	Lets you schedule OSS server status polling.	Enable—Select this check box to enable OSS Server polling. Interval—Enter the interval, in minutes, between each OSS server poll. The valid range is 1 to 10080 minutes.
Redundancy Status	60 minutes	Lets you schedule redundancy status polling of primary and secondary controllers.	Enabled—Select this check box to enable Redundancy status polling. Interval—Enter the interval, in minutes, between each poll.The valid range is 1 to 10080 minutes.
Switch NMSP and Location Status	4 hours	Lets you schedule Switch Network Mobility Services Protocol (NMSP) and Civic Location status polling.	Enable—Select this check box to enable Switch NMSP and Civic Location status polling. Interval—Enter the interval, in minutes, between each poll. The valid range is 1 to 10080 minutes.
Switch Operational Status	5 minutes. Full poll is 15 minutes.	Lets you schedule switch operational status polling.	Enable—Select this check box to enable switch status polling. Interval—Enter the interval, in minutes, between each poll. The valid range is 1 to 10080 minutes. Full operational status interval—Enter the interval, in minutes, between full switch operational status polls. The valid range is 1 to 1440 minutes. Create LinkDown Event—When you enable this feature, Prime Infrastructure generates alarms for both access and trunk ports.
Third party Access Point Operational Status	3 hours	Lets you schedule operational status polling of third party APs.	Enabled—Select this check box to enable third-party AP operational status polling. Interval—Enter the interval, in hours, between each poll. The valid range is 3 to 4 hours.

Table 6-2 Other Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
Third party Controller Operational Status	3 hours	Lets you schedule reachability status polling of third-party controllers.	Enabled—Select this check box to enable reachability status polling of third-party controllers. Interval—Enter the interval, in hours, between status polls. The valid range is 3 to 4 hours.
wIPS Alarm Sync	120 minutes	Lets you schedule wIPS alarm synchronization.	Enable—Select this check box to enable wIPS alarm synchronization. Interval—Enter the interval, in minutes, between each synchronization. The valid range is 1 to 10080 minutes.
Wired Client Status	2 hours.	Lets you schedule wired client status polling.	Enable—Select this check box to enable wired client status polling. Interval—Enter the interval, in hours, between each status poll. The valid range is 1 to 8640 hours. Major Polling—Specify two times of day at which you want to poll all wireless clients for their status. 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 4.2.4 on the Windows NT, Solaris and Linux platforms. The following LMS data can be imported into Prime Infrastructure using the 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, follow these steps:

Step 1 Identify the server where LMS backup data is stored.

Step 2 Open a CLI session with the Prime Infrastructure server (see Connecting Via CLI).

Step 3 Enter the following commands to configure the backup location:

```
admin# configure terminal
admin(config)# repository carsapps
admin(config-Repository)# url location
admin(config-Repository)# user root password plain pword
admin(config-Repository)# end
```

where:

- ***location*** is a fully qualified URL, including access protocol, for the location of the LMS backup data. For example: `ftp://10.77.213.137/opt/lms`, `sftp://10.77.213.137/opt/lms`, or `fdisk:foldername`.
- ***pword*** is the root user password.

Step 4 Import the LMS backup into Prime Infrastructure using the following command:

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

Step 5 Exit your CLI session, log back in to the Prime Infrastructure user interface, and verify that your LMS data was imported properly. The following table shows where to look in Prime Infrastructure for the imported LMS data.

LMS Data	Prime Infrastructure Location
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