Data Collection and Background Tasks

This section contains the following topics:

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 About 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.

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.

About Historical Data Retention

Prime Infrastructure retains two types of historical data:

1. 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.

Note You can define a retention period (and other settings) for each non-aggregated data collection task. For example, you can define the retention period for client association history in **Administration** > **Settings** > **System Settings** > **Client**. By default, the retention period for all non-aggregated historical data is 31 days or 1 million records. This retention period can be increased to 365 days.

1. 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.

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.
- Network audit records: This includes audit records for configuration changes triggered by users, and so on.
- Performance: This includes Assurance data such a traffic statistics, application metrics, and voice metrics.
- System health records: This includes most data shown on Prime Infrastructure administrator dashboards.

The retention periods for these aggregation types are defined as Default, Minimum, and Maximum (see the table below). Use the **Administration** > **Settings** > **System Settings** > **General** > **Data Retention** page to define aggregated data retention periods. Aggregation types include hourly, daily, and weekly.

Table 1: Retention Periods for Aggregated Historical Data

Trend Data Retention Periods			
Period	**Default**	**Minimum**	**Maximum**
Hourly	7 days	1 days	31 days
Daily	90 days	7 days	365 days
Weekly	54 weeks	2 weeks	108 weeks
Device Health Data Retention Periods			
Hourly	15 days	1 day	31 days
Daily	90 days	7 days	365days
Weekly	54 weeks	2 weeks	108 weeks
Performance Data Retention Periods			
Short-Term Data	7 days	1 day	31 days‘
Medium-Term Data	31 days	7 days	365 days
Long-Term Data	378 days	2 days	756 days
Network Audit Data Retention Period			
All audit data	7 days	7 weeks	365 days
System Health Data Retention Periods			
Hourly	7 days	1 day	31 days
Daily	31 days	7 days	365 days
Weekly	54 weeks	7 weeks	365 days
User Job Data Retention Periods			
Weekly	7 days	2 days	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.

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)

Specify 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 Prime Infrastructure 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. The Optical Devices category is not applicable for Prime Infrastructure.

We strongly recommend you to 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.

Specify Client Data Retrieval and Retention

Administrators can use Prime Infrastructure's Client page to configure parameters affecting retention of data on network clients, including:

- Data on disassociated clients. The default is seven days, and this applies irrespective of whether the clients will ever attempt to associate again.
- Data on client session histories. You can also specify the maximum number of session entries to keep, specified as rows in the Prime Infrastructure database.
- Cached client host names retrieved from a DNS server.

In addition to these data-retention options, the page allows you to enable and disable options to:

- Automatically troubleshoot clients using a diagnostic channel when traps are received from these clients.
- Automatically retrieve client host names from a DNS server.
- Poll clients when traps or syslogs are received from these clients
- Discover clients from enhanced client traps.
- Discover wired clients on trunk ports .
- Save as Prime Infrastructure events routine client association and disassociation traps and syslogs. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option at all other times.
- Save all 802.1x and 802.11 client authentication-failure traps as Prime Infrastructure events. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option if your network is stable.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **Client and User** > **Client**.

Step 2 Under Data Retention, modify the values as required.

Step 3 Click Save.

Enable Data Deduplication

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

- Application Response Time data for TCP applications
- Traffic analysis data for all applications
- Voice/Video data for RTP applications

Prime Infrastructure stores all data it receives about network elements and protocols, including any duplicate data that it may receive from multiple sources. When you specify authoritative data sources, only the data from the specified sources is displayed when you view a particular location or site.

The Data Deduplication page allows you to specify one or more authoritative data sources at a specific location. 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 choose to have Prime Infrastructure display only the NAM or the NetFlow data for that location.

Step 1 Choose **Services** > **Application Visibility & Control** > **Data Deduplication**.

Step 2 Select the **Enable Data Deduplication** checkbox and click **Apply**. The Data Deduplication page displays the list of your defined location groups.

Step 3 To automatically detect authoritative sources at all locations, click **Auto-Detect**. If it can identify them, Prime Infrastructure will fill in the address of an authoritative source in the list box under the column listing sources for each of the classes of application data.

Step 4 To specify authoritative sources for a class of application data at a specific location:

a) Click the location group name.

b) Click the drop-down list box under the class of application data for which you want to specify an authoritative source (for example: click in the list box under “Application Response Time”).

c) From the drop-down list, select the data sources you want to specify as authoritative for that location and application data type. Then click **OK**.

d) Click **Save** to save your selections.

Repeat this step as needed for each location and application data type for which you want to specify authoritative data source.

Step 5 When you are finished, click **Apply** to save your changes.

Control 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** > **Settings** > **System Settings** > **General** > **Report** . The Report page appears.

Step 2 In **Repository Path**, specify the report repository path on the Prime Infrastructure server.

Step 3 In **File Retain Period**, specify the maximum number of days reports should be retained.

Step 4 In the **External Server Settings** section, provide SFTP details such as **Server Host**, **Server Port**, **User Name**, **Password**, and the **Repository Path** (where the reports need to be stored in the external server).

Step 5 Click **Save**.

Specify 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** > **Settings** > **System Settings** > **Inventory** . The Inventory page appears.

Step 2 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 3 Select the **Enable Syslog and Traps on device** check box to allow Prime Infrastructure to enable syslog and trap notifications on newly added devices.

Note This feature is not supported on the Cisco Nexus devices.

Step 4 Click **Save**.

Control 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, as explained in the following related topics.

Related Topics

Archive Device Configurations Before Template Deployment, on page 7
Roll Back Device Configurations on Template Deployment Failure, on page 8
Specify When and How to Archive WLC Configurations, on page 8

Archive 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** > **Settings** > **System Settings** > **Inventory** > **Configuration**.

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

Step 3 Click **Save**.

Related Topics

Roll Back Device Configurations on Template Deployment Failure, on page 8

Roll 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 > Settings > System Settings** > **Configuration**.

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

Step 3 Click **Save**.

Specify When and How to Archive WLC Configurations

By default, Prime Infrastructure keeps a backup archive of startup 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

Prime Infrastructure provides configuration archive support for devices running Cisco WLC software. The configuration archive includes only startup configurations. The running configurations are excluded from configuration archive.

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

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

Note The option of masking the security content while exporting is included in the **Inventory > Device Management > Configuration Archive** page. See Download Configuration Files for more information.

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**.

Alarm, Event, and Syslog Purging

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

Prime Infrastructure stores a maximum of 8000000 events and 2000000 syslogs in the database.

To protect system performance, Prime Infrastructure 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, Prime Infrastructure 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	30 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. .

Software Image File Purging

Device software image files are not automatically purged from the database. They must be manually removed using the GUI client.

Control System Jobs

Prime Infrastructure performs scheduled data collection jobs on a regular basis. You can change each job's schedule, pause or resume it, or execute it immediately.

Disabling or limiting these System jobs 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.

Related Topics

Schedule Data Collection Jobs, on page 11
Resume Data Collection Jobs, on page 11
Run Data Collection Jobs Immediately, on page 11
About System Jobs, on page 12

Schedule Data Collection Jobs

System jobs run on a regular default schedule, as described in About System Jobs . You can re-schedule them as needed.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs**.

Step 2 Select the category of data collection job you want to re-schedule (e.g., **APIC-EM Integration**, **Assurance and Health Summary**, **Infrastructure**, **Inventory and Discovery**, or **Status and Wireless Monitoring**).

Step 3 Click the check box next to the system job you want to re-schedule.

Step 4 Click **Edit Schedule** and specify the schedule you want the job to run on.

You can select the date and time the job is executed. You can choose to have the job recur on a minute, hourly, daily, weekly, monthly or annual basis. No end time has been specified by default.

Step 5 When you are finished, click **Submit**.

Resume Data Collection Jobs

You can pause any scheduled data collection job, and resume it if already paused.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs**.

Step 2 Select the category of data collection job you want to pause or resume (e.g., **APIC-EM Integration**, **Assurance and Health Summary**, **Infrastructure**, **Inventory and Discovery**, or **Status and Wireless Monitoring**).

Step 3 Click the check box next to the system job you want.

Step 4 Click **Pause Series** to stop the job from executing.

If the job is already paused, click **Resume Series** to resume execution on the current schedule.

Run Data Collection Jobs Immediately

In addition to the steps below, you can run a job immediately by rescheduling it and selecting the time to execute as **Now** and submit. Then select the job and click run.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs**.

Step 2 Select the category of data collection job you want to run (e.g., **APIC-EM Integration**, **Assurance and Health Summary**, **Infrastructure**, **Inventory and Discovery**, or **Status and Wireless Monitoring**).

Step 3 Click the check box to select the system job you want to run immediately.

Step 4 Click **Run**.

About System Jobs

The following table describes the background data collection jobs Prime Infrastructure performs.

Note You must increase the frequency of the Infrastructure and Inventory jobs with caution as it impacts the performance of Prime Infrastructure over a while as these jobs are high I/O intensive operations.

Table 2: Inventory Data Collection Jobs

Task Name	Default Schedule	Description	Editable options
APIC EM Integration Jobs			
APIC-EM Site Sync	6 hours	Schedules synchronization of sites and devices between APIC-EM and Prime Infrastructure.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
APIC Server Status Periodic	5 minutes	Schedules checks on APIC-EM server reachability.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Ping Network Devices	5 minutes	Schedules ICMP Ping reachability and updates the device reachability status and latency time.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
PnP Bulk Import	5 minutes	Schedules bulk import of device profiles from APIC-EM to Prime Infrastructure.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
PnP Status Polling	5 minutes	Tracks the status of the PnP devices created on APIC-EM and adds them to Prime Inventory when successful.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Post PnP Job		Schedules validation of post-PnP configurations on devices.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Assurance and Health Summary Jobs			
AGGREGATION_HEALTH_SUMMARY	Disabled	Aggregates the health scores of device metrics (Routers, Switches and Access Points).	Non Editable
Assurance DataSource Update	Disabled	Synchronizes the list of data sources between two different processes in PI.	Non Editable
Assurance License Update	Disabled	Fetches the devices and AP which netflow associated with it every 12 hours.	Non Editable
Assurance Lync Aggregation	Disabled	Computes the Lync call statistics.	Non Editable
BASELINE_DAILY	Disabled	Aggregates the hourly baseline values to daily values for the application data.	Non Editable
BASELINE_HOURLY	Disabled	Computes hourly baseline data points for application data.	Non Editable
DAHealth_SITE	Disabled	Synchronizes the site rules between two different processes in PI.	Non Editable
HEALTH_SUMMARY_5MIN	Disabled	Computes the health scores for applications.	Non Editable
PushCollectionPlanToDA	Disabled	Pushes the collection plan to DA.	Non Editable
WUserSyncJob_USER	Disabled	Fetches the list of current clients from the Station Cache to update the netflow user cache.	Non Editable
Infrastructure jobs			
Bulk Recompute RF Prediction	15 days	Schedules status polling of Bulk Recompute RF Prediction.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Connected Mobility Reachability Status	5 minutes	Schedules stauts polling of Connected Mobility Reachability	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Controller Configuration Backup	1 day	Displays the controller configuration backup activities.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Data Cleanup	2 hours	Schedules daily data file cleanup.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Device Config Backup-External	15 minutes	Transfers device configuration periodically to 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).
Guest Accounts Sync	1 day	Schedules guest account polling and synchronization.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Index serach Entities	3 hours	Schedules the Index Search Entities job.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mobility Service Backup	7 days	Schedules automatic mobility services backups.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mobility Service Status	5 minutes	Schedules mobility services status polling.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Mobility Service Synchronization	1 hour	Schedules mobility services synchronization.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
On Demand Reports Cleanup	6 hours	Schedules reports cleanup.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Server Backup	1 day	Schedules automatic Prime Infrastructure 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	Runs for Smart License for the default schedule.	Non Editable.
wIPS Alarm Sync	2 hours	Schedules wIPS alarm synchronization.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Inventory and Discovery Jobs			
Autonomous AP Inventory	1 day	Collects inventory information for autonomous APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Switch Inventory	1 day	Collects inventory information for Switches.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless Controller Inventory	1 day	Collects inventory information for Wireless Controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Status Jobs			
Appliance Status	5 minutes	Schedules appliance polling. This task populates the appliance polling details from the Administration > Appliance > Appliance Status page. It also populates information like the performance and fault checking capabilities of the appliance.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Autonomous Client Status	5 minutes	Lets you schedule status polling of autonomous AP clients.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Autonomous AP Operational Status	5 minutes	Schedules status polling of autonomous wireless access points.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Controller Operational Status	5 minutes	Schedules controller operational status polling.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Device Data Collector	30 minutes	Schedules data collection based on specified command-line interface (CLI) commands at a configured time interval.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Identity Services Engine Status	15 minutes	Schedules Identity Services Engine polling.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Interferers	15 minutes	Schedules interferer information collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Learn Unified AP Ping Capability	This Job remains suspended and runs on-demand.	Schedules Unified AP Ping Capability information collection.	Non-Editable.
License Status	4 hours	Schedules the license-status information collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Lightweight AP Ethernet Interface Status	1 minute	Schedules Lightweight AP Ethernet Interface Status information collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Lightweight AP Operational Status	5 minutes	Schedules Lightweight AP Operational Status information collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Lightweight Client Status	5 minutes	Schedules information collection for Lightweight AP Clients from Network.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mobility Service Performance	15 minutes	Schedules status polling of mobility services performance.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mobility Status Task	15 minutes	Schedules status polling of mobility services engines.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
OSS Server Status	5 minutes	Schedules status polling of OSS Servers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Redundancy Status	1 hour	Schedules redundancy status polling of primary and secondary controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Switch NMSP and Location Status	4 hours	Schedules Switch Network Mobility Services Protocol (NMSP) and Civic Location status polling.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Switch Operational Status	5 minutes	Schedules switch operational status polling.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Third Party Access Point Operational Status	3 hours	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	Schedules operational status polling of third party Controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Unmanaged APs	15 minutes	Collects poll information for unmanaged access points.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Wired Client Status	2 hours	Schedules Wireless Client status polling	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless AP Discovery	5 minutes	Schedules Wireless AP discovery.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless Configuration Audit	1 day	Schedules Wireless Configuration Agent audit collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless Monitoring Jobs			
AP Ethernet Statistics	15 minutes	Schedules AP Ethernet statistics collection.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
AP Image Pre-Download Status	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" checkbox should be selected while downloading software to the controller.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Autonomous AP CPU and Memory Utilization	15 minutes	Schedules collection of information on memory and CPU utilization of Autonomous APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Autonomous AP Radio Performance	15 minutes	Schedules collection of information about radio performance information as well as radio up or down status for autonomous APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Autonomous AP Tx Power and Channel Utilization	15 minutes	Schedules collection of information about radio performance of Autonomous APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
CCX Client Statistics	1 hour	Schedules collection of the Dot11 and security statistics for CCX Version 5 and Version 6 clients.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
CleanAir Air Quality	15 minutes	Schedules collection of information about CleanAir air quality.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Client Statistics	15 minutes	Schedules retrieval of statistical information for autonomous and lightweight clients.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Map Info Polling Job	1 minute		Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Media Stream Clients	15 minutes	Schedules collection of information about media stream clients.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mesh Link Status	5 minutes	Schedules collection of status of mesh links.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Mesh link Performance	10 minutes	Schedules collection of information about the performance of mesh links.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Radio Performance	15 minutes	Schedules collection of statistics from wireless radios.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Radio Voice Performance	15 minutes	Schedules collection of voice statistics from wireless radios.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Rogue AP	2 hours	Schedules collection of information about rogue access points.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Switch CPU and Memory Poll	30 minutes	Schedules polling of switch CPU and memory information.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Traffic Stream Metrics	8 minutes	Retrieves traffic stream metrics for the clients.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless Controller Performance	30 minutes	Schedules collection of performance statistics for wireless controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless QoS Statistics	15 minutes	Schedules collection of information QoS Statistics for Wireless Controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

Migrate Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.5 on all 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 How to Connect 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** *password*

admin(config-Repository)# **end**

where:

a. *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 .

b. *password* 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	Inventory > Network Devices
Static Group	Inventory > Network Devices > User Defined Group
Dynamic Group	Inventory > Network Devices > User Defined Group
Software Image Management Repository Images	Inventory> Software Images
User Defined Templates (Netconfig)	Configuration > Templates > Features & Technologies
LMS Local Users	Administration > Users, Roles & AAA > Users
MIBs	Monitor > Monitoring Policies. In the menu, click Add, then select Policy Types > Custom MIB Polling.