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 related data management tasks.

Related Topics

- Specifying Data Retention by Category
- Specifying Data Retention By Database Table
- About Performance Data Retention
- Specifying Client Data Retrieval and Retention
- About Historical Data Retention
- Enabling Data Deduplication
- Controlling Report Storage and Retention
- Specifying Inventory Collection After Receiving Events
- Controlling Configuration Deployment Behavior
- Controlling Data Collection Jobs
- Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure

Specifying Data Retention by Category

Administrators can use Prime Infrastructure's Data Retention page to configure retention periods for the following data categories:

- **Trend Data**: Hourly, daily and weekly aggregated data.
- **Device Health** and **System Health** data: Hourly, daily and weekly data.
- **Performance** data: Short, medium and long-term data.
- **Network Audit** data.

Limiting the amount of data retained can help improve performance and disk storage characteristics. However, for the best interactive graph data views, Cisco recommends that keep the default values.

You can also specify data retention for individual database tables, using maximum age and record attributes. For details, see "Specifying Data Retention By Database Table" in Related Topics.

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

Step 2 Expand the data category for which you want to specify retention-period values.

Step 3 Enter the new values as needed.

Step 4 Click **Save**.

Related Topics

- Specifying Data Retention By Database Table
- About Historical Data Retention
- Specifying Client Data Retrieval and Retention
- About Historical Data Retention

Specifying Data Retention By Database Table

Administrators can use the "Other Data Retention Criteria" section of the Data Retention page to configure retention periods for specific 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.

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

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

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

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

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

Step 5 Click **Save**.

Related Topics

- Specifying Data Retention by Category
- About Historical Data Retention
- Specifying Client Data Retrieval and Retention
- About Historical Data Retention

About Performance Data Retention

When you choose **Administration > Settings > System Settings > General > Data Retention**, you can modify the retention periods for performance data under **Performance Data Retain Periods**. The performance retention values you specify determine the information that is displayed in performance reports and performance dashboards.

For example, if you don't need any historical data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retain Period—1 day
- Medium term Data Retain Period—3 days
- Long term Data Retain Period—7 days

If you specify these settings, all data displayed in performance reports and performance dashboards data will be for the previous 7 days only. When you generate a performance report (for example, **Reports > Reports > Report Launch Pad > Device > Device Health**), even if you select a Reporting Period longer than the last 7 days, the report contains data from the last 7 days only because that is all the data you've selected to retain.

Similarly, if you view a performance dashboard (for example, **Dashboard > Overview > General > Service Assurance**) and select a Time Frame longer than one week, the dashboard contains data from the last 7 days only because that is all the data you've selected to retain.

For device and interface performance data, Prime Infrastructure uses the values specified in the fields under **Device Health Data Retain Periods**.

Related Topics

- About Historical Data Retention
- Specifying Data Retention by Category

Specifying 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
- 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**.

Related Topics

- About Historical Data Retention
- About Historical Data Retention
- Specifying Data Retention by Category
- About Historical Data Retention

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.

   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.

2. 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.
   - Performance: This includes Assurance data such a traffic statistics, application metrics, and voice metrics.
   - Network audit records: This includes audit records for configuration changes triggered by users, and so on.
   - 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 7-1 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

Table 7-1 Retention Periods for Aggregated Historical Data (continued)

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

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 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.

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 > 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 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 > Settings > System Settings** > **Inventory > 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.

Step 4 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, as explained in the following related topics.

Related Topics

- 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 > Settings > System Settings** > **Inventory > Configuration**.

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

Step 3 Click **Save**.

Related Topics

- Controlling Configuration Deployment Behavior

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

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

Step 3 Click **Save**.

Related Topics

- Controlling Configuration Deployment Behavior

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 Choose **Administration > Settings > 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**.

Related Topics

- Controlling Configuration Deployment Behavior

Controlling Data Collection Jobs

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

Disabling or limiting these background data collection 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 Tasks

- Scheduling Data Collection Jobs
- Pausing and Resuming Data Collection Jobs
- Running Data Collection Jobs Immediately
- About Data Collection Jobs

Scheduling Data Collection Jobs

Data collection jobs run on a regular default schedule, as described in the related topic "About Data Collection 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., **Inventory**, **Wireless Poller**, or **Wireless System**).

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. You can also specify end times and dates, and total recurrences.

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

Related Tasks

- Controlling Data Collection Jobs
- Pausing and Resuming Data Collection Jobs
- Running Data Collection Jobs Immediately
- About Data Collection Jobs

Pausing and Resuming 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., **Inventory**, **Wireless Poller**, or **Wireless System**).

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.

Related Tasks

- Controlling Data Collection Jobs
- Scheduling Data Collection Jobs
- Running Data Collection Jobs Immediately
- About Data Collection Jobs

Running 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” (see “Scheduling Data Collection Jobs” in Related Topics).

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

Step 2 Select the category of data collection job you want to run(e.g., **Inventory**, **Wireless Poller**, or **Wireless System**).

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

Step 4 Click **Run**.

Related Tasks

- Controlling Data Collection Jobs
- Scheduling Data Collection Jobs
- Pausing and Resuming Data Collection Jobs
- About Data Collection Jobs

About Data Collection Jobs

The following tables describe the background data collection jobs Prime Infrastructure performs.

Table 7-2 Inventory Data Collection Jobs

Task Name	Task Status	Default Schedule	Description
Autonomous AP Inventory	Enabled	180 minutes	Collects the inventory information for autonomous APs.
Switch Inventory	Enabled	Daily at midnight	Collects inventory information for switches.
Wireless Controller Inventory	Disabled	Daily at midnight	Collects inventory information for wireless controllers.

Table 7-3 Wireless Poller Data Collection Jobs

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 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.
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.
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.
Traffic Stream Metrics	Enabled	8 minutes	Retrieves traffic stream metrics for the clients.

Table 7-3 Wireless Poller Data Collection Jobs (continued)

Task Name	Task Status	Default Schedule	Description
Wireless Controller Performance	Enabled	30 minutes	Collects performance statistics for wireless controllers.
Wireless QoS Statistics	Enabled	15 minutes	Collects Air Time Fairness statistics.

Table 7-4 Wireless System Data Collection Jobs

Task Name	Task Status	Default Schedule	Description
Interferes	Enabled	15 minutes	Collects information about the interferers.
Mobility Service Performance	Enabled	15 minutes	Collects information about the performance of mobility service engines.
Unmanaged APs	Enabled	15 minutes	Collects poll information for unmanaged access points.

Related Tasks

- Controlling Data Collection Jobs
- Scheduling Data Collection Jobs
- Pausing and Resuming Data Collection Jobs
- Running Data Collection Jobs Immediately

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 > Settings > System Settings > Background Tasks**, then clicking the hypertext link for that task.

Table 7-5 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.

Table 7-5 Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
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.
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.

Table 7-5 Background Tasks (continued)

Task Name	Default Schedule	Description	Editable Options
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.
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 7-5 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 7-5 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 7 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 60 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—Select this check box to have Prime Infrastructure generate 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 7-5 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.

Related Tasks

- Controlling Data Collection Jobs
- About Data Collection Jobs

Migrating Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.5 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 “Connecting Via CLI” in Related Topics, below).

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:

- ***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`.
- ***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.

Related Topics

- Connecting Via CLI