CHAPTER 8

Getting Diagnostic Information from Event Logs

Clients report end-user and power-state actions in log files, which you can display from the Administrator console. Each logged action is referred to as an event. You can use event logs to determine whether policies are effective and to detect and resolve errors.

- Data Tention in Device Logs, page 8-1
- Specifying Server Logging Levels and File Sizes, page 8-4
- Displaying Event Data in the Administrator Console, page 8-6

Data Tention in Device Logs

- Event Categories and Types, page 8-1
- Data Retention, page 8-3
- Log File Locations, page 8-3
- Server File Locations, page 8-3

Event Categories and Types

When you see data logged from system or user activity, you can filter it to select a specific *event category*. The view is broken down by *event types* for the selected category. Event types represent the specific actions or errors that occurred, such as power-state changes to sleep or wake, a user action that delayed a power-state change, and so on.

The following table lists the event categories and describes the event types logged under each.

Table 8-1 Event Categories and Types

Category	Description
Admin Actions	Includes all manual transitions to low-power states that an administrator sets on devices. For example, selecting a set of devices in the Administrator console, right-clicking, and selecting Sleep, Shutdown, or Restart.
Idle Timer Actions	Changes to low power states that occur specifically when the client is inactive (idle) for the length of time set in the assigned policy.

Table 8-1 Event Categories and Types (continued)

Category	Description
Policy Actions	Includes actions that occur through power state transition manager (PSTM) rules. For example, a PSTM rule can terminate a running application before it changes the client to low power, or it can veto the power-state change. event logs record both of those actions. Other events recorded in this category include initial power scheme value when the client service is started, when a power scheme is set according to the policy schedule, when a scheme is set by the user (because the scheme is created to allow the user to override it), and so on.
Scheduled Actions	Any power-state change that occurs according to the schedule set in the policy assigned to the client.
Service Events	Events logged by the client service, such as start, stop, or device check in. Events also include new database creation, and if data collection stops or starts for power state changes and user activity.
State Changes	Detailed power state change data and the request source (Orchestrator server, a third party, or an unknown trigger). Also includes display-only logs for power-state changes.
User Actions	Actions that users take on power schemes or power-state change notifications. For example, omitting or delaying a power-state change or changing the power scheme in the Windows Control Panel. **Note** End users have access to these policy options only if your administrator enables them when configuring the policy in the Administrator console.
User Activity	Events that show whether a user is active or not, whether a transition to a low power state based on idle time is pending, and if user activity is unknown (in which case data and activity collection might have stopped, which generates an event in the Service Events category).
Configuration Errors	Error setting, querying, or deleting a power scheme; changing wake settings on mouse, keyboard (including whether it is a USB device); or loading, parsing, or saving configuration files.
Policy Errors	Errors that prevent a PSTM rule from running. For example, PSTM does not veto a power state change, end an application, or report that an application has ended.
Service Errors	Errors that cause the client service to stop running properly. For example, the client computer loses power; the service does not parse or run a request from the power management service; performance counter for the idle timer is missing or failed; errors that occur during the user or display state queries.
Transition Errors	Problems that occur when the API for a power state transition is called but returns a failure code; errors occurring while processing a power state transition; failure to dispatch a Wake on LAN magic packet; unexpected errors while trying to prevent narcolepsy (computer transition to sleep while in use).
EnergyWise Power Level	Events that occur in the setting or operation of any of the EnergyWise power levels.

If you want to make the event report display more detail, you can combine the event category filter with any of the other standard filters for searching. For example, see successful transitions for a particular policy or user actions in a particular device group or subnet.

Data Retention

The historical period for which you can report on events depends upon a variety of system factors: the number of devices being managed, the reporting interval, the database server hardware, and so on. They determine the rate at which events are generated and the speed at which the database processes large numbers of events.

Under reasonable circumstances, you should be able to see events for 2 to 7 months in the past. However, you might need to trim the data sooner to achieve acceptable performance.

The Orchestrator database contains a table for all events and a separate table for PC power state and user activity events. The latter events are kept for a longer time than error events. Error events are generally used for troubleshooting and resolved relatively shortly after a problem occurs.

Log File Locations

The PC client agent logs event data to a file called PwrMgrService.log in the Orchestrator program directory on the client computer C:\Program Files\Cisco Systems\EnergyWise Orchestrator Agent\Logs.

On 64-bit versions of Windows, Orchestrator Agent folders and files are under Program Files (x86).

Server File Locations

Table 8-2 lists the locations in which you can find log files that contain status and diagnostic information for the Orchestrator server components.

When a new log file is created, the date is appended to the existing log file name, for example, PMPWebService.yyyy.mm.dd.log. The most current log takes the base file name.

Table 8-2 File Locations

Server Component	Path to Log Files
PMP web service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\PMPWebService.log
Enterprise power management service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\PowerManagementProcessor.log
Administrator web service	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\AdminWebService.log
ActiveMQ	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\activemq-5.3.0\bin
EnergyWise proxy service	C:\Program Files\Cisco Systems\EnergywiseProxyServer
The summarization process for reporting (DataSummarization.exe)	C:\Program Files\Cisco Systems\Cisco EnergyWise Orchestrator\Logs\GeneralRepo.log

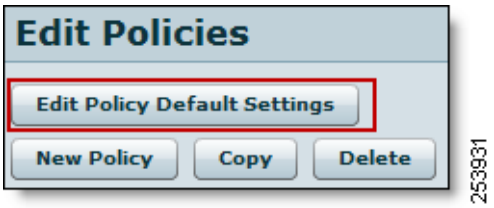
Note The Sustainability Dashboard does not create log files.

Specifying Server Logging Levels and File Sizes

This procedure contains steps for settings for server logging level and log file size, to set policy default settings or override the defaults in individual policies.

Step 1 In the Administrator console, click the **Policies** menu button bar.

Step 2 On the Manage Policies page, click **Edit Policy Default Settings**.



Step 3 On the Data Collection tab, select the default logging level that you want for all policies that you create.

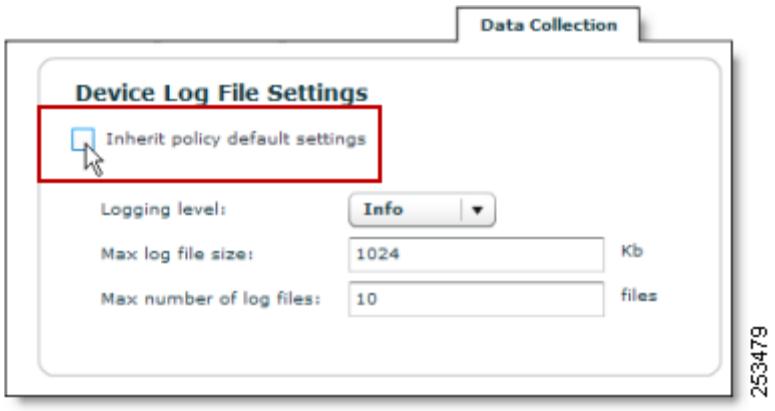
- Info—Informational messages, warning messages, and error messages
- Warning—Warning and error messages
- Error—Only error messages
- Trace—The most verbose and frequent logging
- Debug—A level of logging to use to troubleshoot a particular issue. Only use this on a small set of clients at a time and only under the direction of a Technical Support representative.

Step 4 Select the remaining device log file and data settings.

Setting	Value
Max log file size	Sets the maximum size of log file that you want to maintain. When the current log file reaches that size, Orchestrator creates a new file for subsequent messages, until that file reaches the maximum size, and so on.
Max number of log files	Sets the maximum number of log files to store on client machines.When the maximum is reached, the oldest file is deleted to make room for a new file.
Collect power state data	Select to record power state change events, including successful changes and change errors.
Collect user activity data	Select to record user activity events. Includes actions such as delaying or omitting a power state change or using the Windows Control Panel to change the power scheme from that set by Orchestrator.

To access these settings in an individual policy, on the Policies menu, choose **Manage Policies**, and click the **Data Collection** tab (Figure 8-1). Clear the **Inherit policy default settings** check box, and specify the log settings.

Figure 8-1 Data Collection Tab



When you change policy default settings, all policies that you create after the change inherit those settings by default. If you want a policy to have its own wake or data collection settings, you can change those settings within the policy itself.

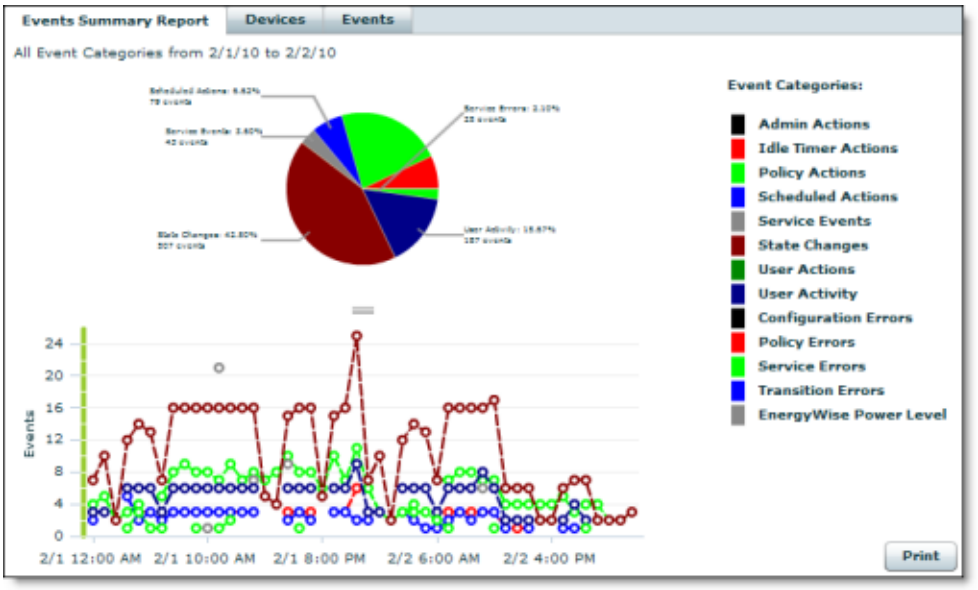
Note If you change these settings in an individual policy, it does not inherit future changes that you make to the policy defaults.

Displaying Event Data in the Administrator Console

You can see client agent activity in a summary report, see a list of devices by event, or see events by event type. You can use search filters to fine-tune the data, for example, to see events only in a particular administration group, events to which a particular policy is assigned, and so on.

1. In the Administrator console, on the Reports menu, click **Events Summary Report**.

   A chart appears, showing events from all event categories, by hour, over the past day. Charts represent the event categories, graphs represent the number of events, and lines represent event categories.



2. To fine-tune the data shown or see the same data differently, choose any process or a combination:

Table 8-3 Displaying Event Data

To Display	Do This
More detail about a part of the chart in the report	Hover the cursor over the section of a pie chart or on a bar chart data point.
All of the event types that occurred within an event category	Double-click the event category in a pie chart. A new chart appears, showing event types within that category.
Information from devices based on particular device attributes	Use the device filters on the left to refine the results by administration group, policy, device family, or subnet. Enter a search string to filter by device name or description.
Events reported by a particular device	In the Event Summary report, click the Devices tab. Click Customize View to add or remove columns.

Table 8-3 Displaying Event Data (continued)

To Display	Do This
All events that occurred on each device or on a specific device, how many times a particular event was logged, and when it occurred	In the Event Summary view, click the Events tab.
A different chart	Select a specific category in the Event category drop-down list.

Variations and Tips

To analyze power-state transitions for one specific device, enter the device name in the Search box, and enter the start and end dates.

See changes by day for a larger set of devices or for longer date ranges. Click column headings to sort by other parameters.

Search Phrase Tips

Search phrases that you enter are not case sensitive.

Orchestrator returns results that contain the search string. Wildcard characters * and ? are processed as text characters, not as wildcards.

For information about seeing devices in the Administrator console, see the "Viewing Devices and Attributes" section on page 4-14.