This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Administrator Extension Help

Centralized Logs

4/25/2025

Centralized Logs

Contents

The Centralized Log Database contains log messages generated by Genesys applications. The Centralized Log plugin for Genesys Administrator Extension displays a summary of those logs, from which you can select and investigate any that are of special interest. As with all objects in GAX, you can only see those logs for which you have the required privileges.

> ### Important
> The Centralized Log Database supports only the Oracle, Microsoft, and PostgreSQL DBMS; IBM DB2 is not supported.

Log messages stored in the Centralized Log Database are of two types:

- Application logs: Generated by most Genesys applications, these logs feature the same unified log record format.
- Audit logs: Generated by only a few applications (notably Configuration Server and Solution Control Server), these logs contain additional attributes and information about configuration changes and control actions performed for processes, solutions, and alarms.

To view the Centralized Log, select **Centralized Logs** in the GAX menu bar.

Centralized Log Window

Log records are displayed in the Centralized Log window.

In the window, the menu on the left shows the views that are available for display, including any Saved Searches.

> ### Important
> Audit Logs are displayed only in the Audit view, and in the results of any searches where the **Type** criteria is set to `Audit`.

Above the list of logs, the following information and controls appear:

- The number of logs that have been retrieved, and the total number of logs to be retrieved. To minimize any delays caused by retrieving all records from a Log Database that contains a huge number of records, records are retrieved in batches from the Database (default batch size is 100); more records are retrieved when you have scrolled halfway through the existing list. In addition, to increase performance, the number of records that can be displayed by GAX is limited (default number of records is 5000). If these parameters are not adequate for you, you can change them using the **minlogs** and **maxlogs** options (respectively). Refer to the "clog Section" of the *Genesys Administrator Extension Deployment Guide*.
- Search criteria used to select the logs in the list. By default, only logs generated on the current day (**Date Range:** Today) are selected. See Filtering Logs for more information about selecting logs using

filters.

- Four control icons:
    - ☰ Opens the search window, in which you set filters to create the list of logs in which you are interested, or at least reduce the list down to a more manageable size.
    - 🗑 Removes selected logs from the list. To select a log for deletion, select the check box in the first column. Select as many as required, or select the check box in the header row to select all of the displayed records.

      > **Warning**
      >
      > If you select the check box in the header row, you will also be prompted to select all records in the database (not just the displayed records) that meet the same criteria as the displayed records. Choose this option ONLY if you are sure that you want to select for deletion all the records in your database that meet those criteria.

    - ▥ Enables you to select what columns (attributes) are displayed in the list.
    - ↻ Refreshes the display.
- Quick filter box—Enter text in this box to search for specific logs without using the full filter capability. Those logs containing that text (including numbers, such as the log ID) will be returned and listed. This filter is case-insensitive, and is cumulative—the query is evaluated and performed, and the list of results is updated as you type each character. For best results, enter as many characters as you can.

Each log record is displayed with some or all of its attributes, as follows:

- **Level**—The log level of the log, either Alarm, Standard, Interaction, or Trace.
- **ID**—The unique identifier of the log, in the format `<Application id>-<message ID>`, where <Application ID> is the Application ID of the Application that generated the log, and <message ID> is the numeric identifier of the log message, unique within the component that generated the log.
- **Description**—The text of the log message.
- **Host**—The host on which the Application that generated the log was running.
- **App**—The name of the Application that generated the log.
- **Date**—The date and time when the log was generated.
- **Interaction ID**—The identifier of the interaction for which this log was generated. This attribute appears only for Interaction-level logs.

You can also click ▥ and customize what attributes (columns) are displayed; by default, all columns are displayed.

The actual attributes displayed depends on the selection made in the menu on the left of the window, and on the attributes that you have chosen to display. For example, the **Level** attribute is not displayed if you have selected to display only Standard-level logs.

Click in the line of any log to see additional attributes.

Viewing Logs

In the Centralized Log window, you can:

- View all Application-type logs, by selecting **All Logs** under **Applications** in the left-hand menu.
- View all logs of a certain level, by selecting the appropriate level under **Applications**. For example, to view all Standard-level Application logs, select **Standard** under **Applications**.
- View all Audit-type logs, **All Logs** under **Applications** in the left-hand menu.
- View all logs meeting criteria defined in a saved search, by selecting the search name under **SAVED SEARCHES** in the left-hand menu.
- Create a new search for all logs meeting specified criteria, by filtering the logs based on specified criteria.

By default, GAX displays the logs sorted by their **Date** attribute. You can sort also them by their **Level**, **ID**, **Description**, **Host**, **App**, and **Date** (and time) when they were generated. Click in a header cell to sort the list by that attribute and/or to change the order of the list (ascending or descending).

Searching for Logs

You can search for specific logs by filtering a list of logs by one or more search criteria. Click to open the filter window. From this window you can perform a Basic Search or an Advanced Search:

- Basic search—Enables you to view a subset of the logs using a basic set of criteria.
- Advanced search—With specified privileges, enables you to filter the list using additional criteria, save the searches, manage the list of saved searches, and remove some or all of the logs.

Click **Save As** to save up to 10 defined searches, for use at a later time. If you want to save a new search but have already saved 10, you must delete one of the existing searches (click the **x** that appears when you hover the mouse on the search name) before saving the new one. You can also drag the search names up and down to reorder them in the list.

Tip

- Before starting your search, be sure that all log records have been retrieved from the database—check the record count in the top right corner of the Centralized Log window.
- If all you want to do is search for log records containing some text, or even a log record

> with a unique ID, you can most likely get the same results as a Basic or Advanced Search by entering the text in the Filter Table box at the top-left of the window.

Basic Search

In a basic Search, you can filter logs based on **Host**, **Application**, **Tenant**, **User**, **Date**, and/or **Description**.

Note the following when performing a basic search:

- You can enter only one filter value for each attribute.
- The **Host**, **Application**, **Tenant**, and **User** filters contain drop-down lists of the values of the corresponding attribute for each log record in the original list.
- The **Date** filter includes eight predefined filter values, as follows:
  - `Last 5 Minutes`
  - `Last 15 Minutes`
  - `Last 1 Hour`
  - `Today`
  - `Yesterday`—Current and previous days
  - `Last 5 Days`—Current and last 5 days
  - `Last 30 Days`—Current and last 30 days

  All days start at midnight (00:00:00); minute and hourly intervals are measured from the time when the filter is run.

  You can also select **Custom Date Range** and select a range of dates and times in the adjacent calendars that appear.
- The **Description** filter has no drop-down list; enter any text that might be found in the **Host name**, **Application name**, or **Description** of the log. This is somewhat different from the **Quick Filter** box located above the record list, in that this field looks only for matching text in three attributes, so cannot be used to look for a log of a given number.

To filter the logs, select a value for one or more search criteria, and click **Search**. The logs that meet the specified criteria are listed.

Advanced Search

To use the Advanced Search filter, you must have the ACCESS_CLOGS privilege. This advanced filter gives you more search criteria, and if you have the DELETE_CLOGS privilege, you can also delete from the Centralized Log Database some or all of the log records returned by your query.

To define an Advanced filter, first enter any filter criteria for a Basic Search. Then click the arrow next to Advanced Search. The Search window expands to show the additional filters with which you can search for logs, specifically:

- **Log Type**—`Application` or `Audit`
- **Log Level**—`Alarm`, `Standard`, `Interaction`, or `Trace`
- Name of **Solution** in which the log was generated.
- Type and name of configuration objects that have been changed.
- Key name and value of attributes that have been changed.

To clear a value from a filter, click **Reset**; to clear all filters click **Reset All Filters**. To remove only some of the Key:Value pairs entered in the **Attributes** filter, click the adjacent 🗑 .

In the list of records returned by the Advanced Search, you can view and sort the log records as usual. Click 🗑 to delete selected records from the Centralized Log Database. (You must have the DELETE_CLOGS privilege to delete records.)

Log Levels

Genesys Administrator reports log events at four levels of detail: Alarm, Standard, Interaction, and Trace. Log events of these levels feature the same unified log record format and can be stored in the Centralized Log Database.

In addition, some applications also generate Audit logs. These Audit logs usually contain additional attributes and information about configuration changes and control actions performed for processes, solutions, and alarms.

Alarm Level

Alarm-level logs contain only log records of the Alarm level. Solution Control Server (SCS) generates Alarm log events on behalf of other applications when receiving from them log events configured as Detection Events in Alarm Conditions. Using this level, SCS reports the occurrence and removal of all alarms to the Centralized Log Database.

Standard Level

Standard-level logs contains high-level events that report both major problems and normal operations of in-service solutions. An event is reported at the Standard level if it satisfies one of these criteria:

[+] Show criteria

- Indicates that an attempt to perform any external operation has failed

- Indicates that the latest attempt to perform an external operation that previously failed has succeeded
- Indicates detection of a condition that has a negative impact on operations, actual or projected
- Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
- Indicates a security violation of any kind
- Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
- Indicates inability to process an external request
- Indicates successful completion of a logical step in an initialization process
- Indicates a transition of an application from one operational mode to another
- Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
- Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range

Interaction Level

Interaction-level logs report the details of an interaction processed by solution components that handle interactions. The log contains information about the processing steps for each interaction by each solution component. An event is reported at the Interaction level if it:

- Is a recognizable high-level data exchange with another application about an interaction.
- Indicates a change in real-time state of an interaction handled by the application (unless such a change is visible from the high-level data exchange).

The specific criteria depend on a particular component and its role in interaction processing.

Trace Level

Trace-level logs report the details of communications between the various solution components. The log contains information about the processing steps for each interaction by each solution component. An event is reported at the Trace level if it satisfies one of these criteria:

- It is a recognizable high-level data exchange with another application.
- It is a recognizable high-level data exchange with an external system.
- It indicates a change in real-time state of user-level objects that the application handles (unless such a change can be seen from the high-level data exchange).

For More Information

For more information about logging in Genesys software, refer to the *Framework 8.5 Management*

Layer User's Guide. For descriptions of the logs themselves, refer to *Framework Combined Log Events Help*.