Framework Management Layer User's Guide

How to Set Up and Use an Audit Trail

4/25/2025

How to Set Up and Use an Audit Trail

Contents

You can use Management Layer's centralized logging functionality to set up an audit trail using audit logs.

Setting Up the Audit Trail

Audit logs are log messages of type Standard or Trace that are marked as audit-related, and are logged in response to some action or event that requires an audit. To determine which logs are actually Audit logs, refer to *Framework Combined Log Events Help*. This help file identifies Audit logs for each component.

To set up the Audit trail, use the log configuration option **verbose**, and set the output to `network` to ensure that the logs will be stored in the Log Database, ready for viewing.

For more information about the options used in setting up an audit trail, refer to the *Framework Configuration Options Reference Manual*. For more information about log levels, see Log Levels.

Standard-Level Audit Logs

To set up an Audit trail using only Standard-level Audit logs, configure the following options:

- In the Application objects representing the components that have Audit logs and for which you want to set up an audit trail:

  ```
  [log]
  verbose=standard
  standard=network
  ```

  and optional, but recommended:

  ```
  print-attributes=true
  ```

- In Message Server:

  ```
  [messages]
  db-storage=true
  ```

This will ensure that log events of Standard level will be stored in the Log Database, ready for viewing. Use the *Framework Combined Log Events Help* to identify which of the logs are Audit logs.

Standard- and Trace-Level Audit Logs

> **Warning**
> Trace-level logging generates a significantly greater number of logs than Standard-level logging, and may affect the performance of your system.

To set up an audit trail with Standard- and Trace-level Audit logs, configure the following options:

- In the Application objects representing the components that have Audit logs and for which you want to set up an audit trail:

```
[log]
verbose=trace
trace=network
```

and optional, but recommended:

```
print-attributes=true
```

- In Message Server:

```
[messages]
db-storage=true
```

This will ensure that log events of Standard, Interaction, and Trace level will be stored in the Log Database, ready for viewing. Use the *Framework Combined Log Events Help* to identify which of the Standard- and Trace-level logs are Audit logs.

Viewing Audit Logs

You can view Audit logs using Genesys Administrator. Do the following:

1. In Genesys Administrator, select **Monitoring > Environment > Centralized Log**, and select the **Audit** tab.
2. To view a single Audit log record, click the small triangle to the left of the record.
3. To view all Audit log records for a specific application or host, do one of the following:
   - Filter these records by entering the name of the application or host in the **Application** or **Host** field, respectively. If the **Filter** panel is not visible, click the binoculars icon in the far right end of the Filter bar.
   - Select **Provisioning > Environment > Applications or Hosts> <name of object>**, and select the **Audit** tab.

For more information, refer to *Genesys Administrator Help*.