Relativity Metrics Guide

May 20, 2024 | Version 12.3.805.2

Table of Contents

1 Telemetry

Telemetry is a required Relativity application that collects metrics:

- **System usage metrics** – Telemetry collects system usage metrics and securely sends the data to Relativity to improve the quality and performance of Relativity applications.

- **Billing data** – Telemetry also collects and sends billing data to Relativity.

Telemetry collects billing data and system usage metrics with the Billing Agent. For more information, see Billing Agent.

1.1 Configuring telemetry

All versions of Relativity:

- Billing Agent must be running.

- The server hosting the Telemetry Metrics Transmission agent must be able to send outbound HTTPS requests to **update.kcura.com**. If necessary, make necessary changes to your firewall settings.

- The Telemetry Metrics Transmission agent must be running. It is automatically added to the Agents tab at the instance level. The agent uses the same setup as your Billing Agent server and resource pool configuration.

You can use the Telemetry Smoke Test Relativity script to verify that telemetry is properly configured in your environment.

1.2 Configuring metrics collection

You can configure the metrics that you want to collect by updating specific values for instance settings, and running scripts to enable the collection of metrics for specific applications.

1.2.1 Enabling metrics categories

Depending on the version of Relativity, you can enable specific metrics categories and exclude the ones you don't need.

The settings in the EDDSMetrics.Whitelist table control whether Relativity collects metrics for a specific application, for example, Processing. This table is added to your Relativity environment when you install Relativity. It contains all enabled metrics categories. For more information about configuring metrics, contact Relativity Customer Support via the Community site.

1.2.2 Obfuscating metrics

If your company does not need us to include user, case, matter, or client names on your Relativity invoices for your own billing or record-keeping purposes, you can use Relativity instance settings to obfuscate them. Common reasons for not obfuscating include billing users and/or workspaces to your customers and ease of managing your user base. We recommend that you consult with your finance/billing department and those who manage your Relativity user base before making changes to the default values.

The instance settings are as follows:

- ReplaceCaseNameWithArtifactID - determines whether case names are replaced by case artifact IDs.

- ReplaceUserNameWithHashValue - determines whether the username portions of user email addresses are replaced by hash values. If you have multiple Relativity instances, the value of ReplaceUserNameWithHashValue must be the same across all instances in order for us to properly calculate and bill your users.

- ReplaceClientNameWithHashValue and ReplaceMatterNameWithHashValue - determines whether the client and matter names are replaced by hash values

- LockoutNotificationList - Defines the distribution list for emails warning of a case statistics-based or license-based lockout. For more information, see our Community article on setting up billing contacts to receive alerts.

1.3 Telemetry lockout

Telemetry is used to collect and transmit billing data to Relativity. This functionality exists in parallel with Billing Agent.

> **Note:** Failure to transmit telemetry billing data to Relativity causes Relativity access to be disabled after seven (7) days. Telemetry lockout is similar to Billing agent lockout. If your security setup doesn't allow access to public internet, contact Relativity support to configure offline-billing.

A notification of metrics transmission failure is displayed in Alerts:
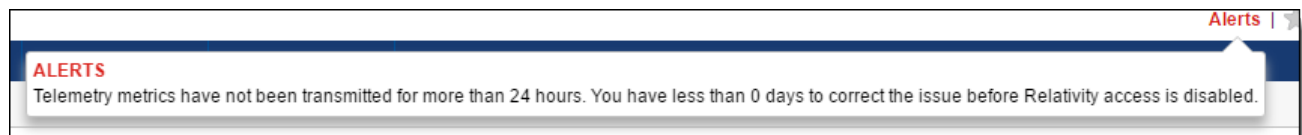
Metrics transmission failure can be caused by network access problems. It can also be caused by Relativity services failures on the telemetry agent server.

To troubleshoot metrics transmission failure:

- Review Relativity logs. Look for error related to Metrics Transmission Agent. In most cases, the error message and the exception stack trace can point you to the cause of the failure. You can also use the Errors tab in Relativity.

- Verify that your network firewall rules allow outbound HTTPS traffic from the Telemetry Transmission agent server to **update.kcura.com.**

- Verify that Relativity services are running properly on the Telemetry agent server and that metrics are being logged.

- Verify that your network firewall rules allow outbound internet traffic from the telemetry agent server to the Relativity billing server.

- After you identified and corrected the problem, the telemetry agent will be automatically rerun and Relativity access will be restored. Note that the Metrics Transmission Agent must be set to Active and the Relativity Agent Manager service must be running.

2 Billing Agent

The Billing Agent, formerly known as Case Statistics Manager agent, collects system usage and billing information for Relativity. This agent must be enabled to keep your Relativity access enabled.

2.1 Billing data settings

If your company does not need us to include user, case, matter, or client names on your Relativity invoices for your own billing or record-keeping purposes, you can use Relativity instance settings to obfuscate them. Common reasons for not obfuscating include billing users and/or workspaces to your customers and ease of managing your user base. We recommend that you consult with your finance/billing department and those who manage your Relativity user base before making changes to the default values.

The instance settings are as follows:

- ReplaceCaseNameWithArtifactID - determines whether case names are replaced by case artifact IDs.

- ReplaceUserNameWithHashValue - determines whether the username portions of user email addresses are replaced by hash values. If you have multiple Relativity instances, the value of ReplaceUserNameWithHashValue must be the same across all instances in order for us to properly calculate and bill your users.

- ReplaceClientNameWithHashValue and ReplaceMatterNameWithHashValue - determines whether the client and matter names are replaced by hash values

- LockoutNotificationList - Defines the distribution list for emails warning of a case statistics-based or license-based lockout. For more information, see our Community article on setting up billing contacts to receive alerts.

You can also use the AgentOffHourStartTime and AgentOffHourEndTime to change the off-hours for running the Billing Agent.

If the billing report queries consistently fail and there are SQL timeout errors in the log, you can use the LongRunningCaseStatisticsQueryTimeout instance setting to increase the timeout value.

2.2 Troubleshooting Billing Agent

Billing Agent failure scenarios include:

- The Billing Agent fails to start.

- Individual SQL methods in the agent timeout resulting in the total failure of the agent.

- The Billing Agent attempts a retry on workspaces that initially failed while still in off-hours and work-space(s) fail again.

2.2.1 Auto-retry

If the Billing Agent fails on a workspace, it moves on to the next workspace. If the agent is still running in off-hours, it retries the workspace(s) that failed. If the workspace(s) still fail, the CSV file is not generated and the billing file is not be produced.

2.2.2 Billing Agent alerts

If Billing Agent fails to complete a report for any of the workspaces in your environment, an alert appears in the Alerts section. The alert lists the failed workspaces and the date the agent failed.

Note: Billing Agent alerts are visible only to admin users.

If workspace count is less than or equal to five (5):

```
The Billing Agent failed for workspaces XXXXXXX, XXXXXXX, XXXXXXX, XXXXXXX,
XXXXXXX on 10/31/2016.
```

If workspace count is greater than five:

```
The Billing Agent failed for 17 workspaces on 10/31/2016.
```

The Billing Agent is not disabled upon failure. The alert will be reset once the agent runs again. Detailed information on Billing errors can be found on the Errors tab. You can find even more granular information in the Relativity logs.

2.3 Restricted Relativity access

If the Billing Agent data is not sent for seven days, Relativity access becomes restricted. Once access has been restricted, only system admins are able to access the system. Other users are locked out. This limited access allows administrators to log in to Relativity and address the problem, for example, by re-enabling the agent.

Once the billing data is sent, access returns to normal.

If the Billing Agent fails to generate and send data for all workspaces during the off-hour run, admin users are notified.

Note: To set or update your billing contact, contact Relativity Support.

Proprietary Rights