



# Monitoring And Log Retention

Every call through the connector is recorded, with both payloads. This is how you read that record, and how you keep it from growing without limit.



Transaction `/CGR/MONI` provides request tracking. Selection criteria isolate specific calls or time windows, and each record in `/CGR/API_LOG` carries a unique `MESSAGE_ID` for application-level tracking.

## WHAT EACH RECORD SHOWS

| Field                                  | Purpose                                                           |
|----------------------------------------|-------------------------------------------------------------------|
| <b>Status</b>                          | Separates successful calls from failed executions                 |
| <b>Date and time</b>                   | Correlates SAP logs with external application timestamps          |
| <b>Object type and name</b>            | Identifies table, function or report requests                     |
| <b>SAP user</b>                        | Shows the technical identity used for authorization checks        |
| <b>Source host</b>                     | Identifies the origin of the HTTP request                         |
| <b>HTTP method and response reason</b> | Distinguishes request shape, authorization and execution failures |



### ONE RECORD, ONE REQUEST

Every call through the connector produces exactly one row, whether it succeeded or failed. There is no sampling and nothing is discarded on the way in.



## Inspecting payloads

- 1 Select a request row in `/CGR/MONI`.
- 2 Choose **Display Request Payload** to see the parameters received.
- 3 Choose **Display Response Payload** to see the JSON returned.
- 4 On a failure, compare the result with backend dumps or authorization logs.



### A DISPLAY LIMIT, NOT A STORAGE LIMIT

The monitor displays only the first 500 records when the stored payload is very large. The stored record itself is complete.

## RETENTION AND CLEANUP

Transaction `/CGR/DELETE_LOG` manages retention. Set the retention period in days, then schedule the cleanup job.

- Coordinate retention periods with application owners and security teams.
- Schedule the job before `/CGR/API_LOG` grows unnecessarily.
- Retain logs long enough to investigate delayed error reports.
- Response payloads may contain personal or otherwise regulated data – set the period to your data-protection policy, and export to file where an external audit trail is required.

### CGR SOFTWARE

Retention questions from your security team are welcome.

cgrsoft.com  
sales@cgrsoft.com