

Configuration

Configure licensing, object definitions, access, routing and optional operational features in the correct SAP client.

Install the license in the application client

1. Give CGR the target licensing system identifier. Basis can obtain the full value from SLIC_GET_SYSTEM_ID, output SYSTEMID; it may differ from the ordinary three-character SAP SID.
2. Receive the original CGR-issued license text file for product SAP_CONNECTOR and that target system.
3. Open /CGR/LICENSE in each application client that will use the Connector. Enter SAP_CONNECTOR in Product and select the license .txt file with the file chooser.
4. Execute and confirm License installed successfully or License replaced successfully. Check product, system identifier and validity date.

The complete license file contains the CGR1 key. Preserve the original file rather than copying an abbreviated value. Replacing a license updates that product in the current client. The Connector performs no outbound HTTP/HTTPS licensing request.

Configure the generic object catalog

In /CGR/BO, create or verify the rows below. Save and record them in a customizing request if your landscape prompts for one.

API BO	Description	POST Input Structure
FUNCTION	Generic Function API	Blank
TABLE	Generic Table API	/CGR/ST_TABLE_INP
REPORT	Generic ALV Report API	/CGR/ST_REPORT_INP

Leave POST Output, PUT Input, PUT Output and GET Output Structure blank for these generic rows. This catalog describes interfaces; it does not grant users access. Removing a catalog row is not a way to revoke an existing API grant.

Grant exact user and object access

Maintain /CGR/API_AUTH in the same client used by the API. Use uppercase SAP user names, API BO values and object names. A matching grant is required; there are no deny overrides.

User (example)	API BO	Object Name	Meaning
CGR_API	TABLE	MARA	This user may request this table
CGR_API	FUNCTION	BAPI_PO_GETDETAIL	This exact function
CGR_API	REPORT	YOUR_REPORT	This exact report program

CGR_API	TABLE	*	All TABLE objects for this user
CGR_ADMIN	*	*	All object types and objects for this user

Wildcard grants are broad

The user must be exact. Only a complete * for Object Name, or * in both API BO and Object Name, is supported. Partial patterns such as BAPI_* or MA*, a wildcard user, and API BO * with a specific object name are not supported. Deleting an exact row does not revoke access while a matching wildcard remains.

Connector grants do not grant SAP transaction or configuration maintenance permissions. Basis must separately assign the appropriate SAP roles for authentication, Gateway scopes, business operations and administrative actions. Metadata access is also authorized; knowing an object name does not grant its definition or execution.

Validate the execution route

Scenario	Configuration and verification
Local SICF execution	Use the local route and verify the application client and logged backend user.
Default SICF backend	Maintain key BACKEND in /CGR/RFC_DEST; verify the destination and actual user mapping.
Selected SICF backend	Use the approved sap-system alias; Basis verifies its RFC destination and identity.
Gateway OData	Register /CGR/CONN_SRV for the intended Gateway system alias; execution stays in the Gateway-selected backend.

The current SICF execution policy requires the observed backend user to match the request user. Do not resolve a mismatch by assuming the original user supplies backend permissions. Validate each route with an allowed and a denied read-only test.

Set logging and retention policy

Versioned settings are client-local in /CGR/CONN_CFG, CONFIG_ID GLOBAL. An absent row supplies the defaults below; an invalid stored row fails validation. There is no general retention-duration maintenance transaction or generated SM30 dialog. Use a controlled client-specific administrative procedure to change durations, validating all fields and change metadata.

Setting	Default	Meaning
HEADER_DAYS	90 days	Completed attempt-chain headers
INPUT_DAYS	7 days	Successful normalized context and original request
FAIL_INPUT_DAYS	30 days	Failed normalized context and original request
RESPONSE_DAYS	1 day	Successful backend output
FAIL_RESP_DAYS	30 days	Failed output or execution diagnostic

Header retention must cover the payload retention durations. Completed records retain their stored deadlines; a later settings change does not recalculate them. RUNNING/UNKNOWN chains are protected for investigation. /CGR/RET_ADMIN controls only the optional manual-cleanup switch; scheduled /CGR/RET_PURGE uses its separate Execute decision.

Configure optional result classification

1. Open /CGR/RES_ADMIN in Preview. Define an exact FUNCTION and output parameter with the BAPI_RETURN evaluator and publish using the current expected revision.
2. Review the profile and deliberately enable classification. Each new attempt captures the configuration revision when it begins.
3. Inspect Classification in /CGR/MONI. Changing a profile affects future attempts; historical results are not reevaluated.

No configuration means classification is off. Profiles interpret complete typed output; missing or inconclusive RETURN evidence yields UNKNOWN. TABLE and REPORT have technical outcomes only. Classification never changes HTTP status, business commit policy or rerun eligibility.

Configure notifications and digests

1. In /CGR/NTF_ADMIN, configure the exact object, outcome, rule, verified sender and recipients. Choose INDIVIDUAL or DIGEST, then deliberately enable capture. Business-result rules need the appropriate classification profile.
2. In /CGR/NTF_DLV_ADMIN, preview the admission revision and set a prospective UTC cutoff through PAUSED before opening automatic preparation. Preparation does not authorize sending.
3. In /CGR/NTF_SEND_CTL, preview and open sending AUTO using the exact current sending/admission revisions and a future cutoff. The effective cutoff is the later value; old backlog is not adopted.
4. In /CGR/NTF_JOB, preview the proposed periodic job, review the interval (default 15 minutes) and execute with those revisions. Digest interval is a separate setting, also defaulting to 15 minutes.
5. Check SM37, /CGR/NTF_DLV_VIEW and SOST. Basis must configure SAPconnect/SMTP and verify actual mail delivery.

Installation leaves capture and sending disabled and schedules no job. Rule changes apply to new captures; existing intents keep their captured route and content. Revoking AUTO stops new application claims but does not recall SAPconnect mail already queued. Stop an existing periodic job in SM37 when required.

CGR SOFTWARE

cgrsoft.com · sales@cgrsoft.com

Use these release 2.0 instructions with the supplied release delivery notes. Release 1.3 has a separate documentation and PDF set.