

Twenty connector

The Twenty connector exposes a fixed workspace-aware REST surface as governed AIP capabilities. Use it to manage standard or custom records, inspect or change selected workspace metadata, read generated OpenAPI documents, and ingest signed

SECTION	Connectors
TYPE	Connector
PROTOCOL	AIP 1.0
SOURCE	docs/connectors/twenty/README.md

The connector is not an arbitrary HTTP or GraphQL proxy. Provider paths, operation names, query keys, credential placement, request limits, approval, idempotency, retry, response handling, and webhook verification are fixed in source.

Decide whether it fits

Requirement	Fit
Query standard and custom object records	Yes
Create, batch upsert, update, soft-delete, destroy, restore, or merge records	Yes, through fixed operations
Find duplicates or run provider-native group-by	Yes
Manage object, field, view, layout, and webhook metadata	Yes, for twelve allowlisted resources
Read workspace-specific core and metadata OpenAPI documents	Yes
Receive signed Twenty webhook events through AIP	Yes, when ingress security and event delivery are configured
Call arbitrary REST paths	No
Execute arbitrary GraphQL	No
Create or expose Twenty API keys	No
Stream, cancel, transact, compensate, or automatically reconcile provider work	No
Prove compatibility with any Twenty revision or deployment	No

Choose a separate, narrowly reviewed connector when an excluded provider surface is required. Do not add a caller-selected path or credential to an Action.

Fix the reviewed identity

Property	Reviewed value
AIP source	97be86e9efedf07ecf1783b03800f683f107fb04
Connector crate	aip-connector-twenty 1.0.0 workspace line
Standalone host	aip-host-twenty 1.0.0 workspace line
Connector profile	aip.connector.twenty.v1
AIP protocol	1.0
Upstream mapping revision	96a24563674313a3071d359bfccaf33d5e130ab8
Operation catalogue	22 fixed operations
Metadata catalogue	12 fixed resources

The upstream commit is the mapping reference recorded by connector source. A deployed Twenty image, edition, migration state, and workspace schema require their own identity and evidence.

Understand the deployment boundary

One standalone `aip-host-twenty` process owns:

- one AIP tenant, connector instance, and concrete replica;
- one configured Twenty workspace UUID;
- one fixed Twenty origin;
- one owner-controlled API-token file;
- one optional owner-controlled webhook-secret file;
- one optional operation allowlist;
- durable AIP runtime, replay, event, and outbox state;
- native AIP signing, lifecycle, routing, and credential-revision policy.

The host receives signed AIP Actions and sends synchronous REST requests with a Bearer header. It disables redirects and adds the AIP Action ID to provider requests.

Keep one host instance bound to one tenant and intended Twenty workspace. The workspace UUID participates in deterministic create IDs, manifest identity, webhook validation, and external-account routing.

Read the capability groups

Group	Operations	Purpose
Record query	4	List, get, find duplicates, and group records
Record create and update	4	Create, create many, update, and update many
Record lifecycle	7	Soft-delete, destroy, restore, and merge
Metadata	5	List, get, create, update, and delete allowlisted resources
OpenAPI	2	Read workspace core and metadata documents

Capability IDs use `cap:twenty:`, such as `cap:twenty:record.list` or `cap:twenty:metadata.update`.

An optional operations file can reduce the 22-operation catalogue. An empty allowlist is invalid. Deployment policy cannot introduce an unknown operation.

Use the fixed record surface

Record Actions name an object matching `^[A-Za-z][A-Za-z0-9_]{0,127}$`. This permits Twenty standard and custom object names without allowing path separators or arbitrary provider routes.

Single-record operations require an RFC 4122 UUID version 1 through 5. Bulk update, soft-delete, destroy, and restore require a non-empty provider filter.

Create and create-many operations force Twenty `upsert=true`. When a body lacks an ID, the connector derives a deterministic UUID version 5 from workspace, idempotency key, and item index.

An explicit valid record UUID is preserved. Batch create accepts one through 200 record objects.

Restore-one uses Twenty's filtered collection restore route because the pinned provider revision rejects the documented single-record restore path. The connector injects an exact ID filter after validating the requested UUID.

Use only allowlisted metadata

The metadata surface includes:

- `objects` and `fields`;
- `views`, `viewFields`, `viewFilters`, `viewGroups`, `viewSorts`, and `viewFilterGroups`;
- `pageLayouts`, `pageLayoutTabs`, and `pageLayoutWidgets`;
- `webhooks`.

Each list resource accepts only its provider-specific query keys. Page-layout tabs require `pageLayoutId`; widgets require `pageLayoutTabId`.

Webhook metadata has an additional secret boundary. Action input cannot supply `secret`. Create injects the configured host secret, and update injects it only when `rotateConfiguredSecret` is exactly `true`.

The connector recursively removes every `secret` key from webhook metadata responses.

Apply governance by operation

Class	Count	Approval	Idempotency	Retry contract	Risk
Reads	8	No connector-required approval	Optional	Safe	Low
Create one or many, update one	3	Required	Required	Safe with key	High
Other record mutations	8	Required	Required	Unsafe	High, except permanent destroy
Metadata mutations	3	Required	Required	Unsafe	Critical

The two permanent-destroy operations are also critical. Every mutation requires tenant-policy approval with reason, input snapshot, and policy decision. Approval expires after 15 minutes.

Mutation idempotency is scoped to the external account, uses input-hash revalidation, and declares a seven-day contract TTL. The connector forwards the key but does not provide a local provider-effect reconciliation API.

All operations are synchronous. The connector publishes no async, streaming, cancellation, transaction, reconciliation, or compensation support.

Interpret retry safety narrowly

The eleven retry-safe operations are the eight reads plus create, create-many, and update-one. The create paths use deterministic IDs and force provider upsert.

Update-many, deletes, restore, merge, and metadata mutations remain retry-unsafe. A 429 or 5xx response marks every mutation outcome uncertain, including a retry-safe mutation.

Transport failure is retryable only when the operation contract permits it and the connector can classify the failure safely. Reconcile the original Action and provider state before retrying any uncertain mutation.

Protect data and credentials

Every capability declares confidential data, possible personal data, and required redaction. Record bodies, query filters, metadata, OpenAPI documents, webhook payloads, and provider errors can expose workspace structure or customer data.

The API token remains in an owner-controlled file and is used only as a Bearer header. It must be UTF-8, at most 16 KiB, and contain no whitespace or DEL.

The webhook HMAC secret is separate. It is injected into webhook metadata only inside the host and never accepted from protocol input.

Provider error output retains only bounded allowlisted fields. Provider request identity accepts a bounded `x-request-id` or `traceparent` value without control characters.

Understand webhook ingress

Webhook ingress is absent unless a secret file is configured. When enabled, the host also requires a central connector-event endpoint.

The fixed route `/webhooks/twenty` requires timestamp, signature, and nonce headers. Verification uses HMAC-SHA-256 over exact bytes:

```
TEXT
<decimal timestamp>:<raw request body>
```

The timestamp must be within five minutes. The signature is 64 hexadecimal characters, and the nonce is 32 hexadecimal characters.

The host validates workspace ID, webhook UUID, RFC 3339 event time, event-name syntax, and JSON object shape. A durable compare-and-swap store admits each nonce once, with a bounded 100,000-nonce window.

An accepted delivery becomes a deterministic AIP event, enters the durable event log, then enters the central outbox. HTTP success reports whether central delivery was newly queued or already present.

Respect the transport bounds

Boundary	Source value
Connect timeout	10 seconds
Complete provider request timeout	120 seconds
Provider JSON body	16 MiB
Default provider response	64 MiB
Maximum configured response	256 MiB
Encoded URL	128 KiB
Query entries	64
One encoded query value	32 KiB
Batch records	200
Webhook body	4 MiB

Response reading is streaming but the AIP operation is not. The connector buffers one bounded JSON response and rejects invalid JSON.

Know the maturity boundary

The reviewed source contains contract tests and a standalone host. Its generic image verifier builds the Twenty host, but the pinned five-product Compose qualification topology does not include a Twenty service.

Local retained evidence may describe another exact Twenty run. It does not qualify an unspecified rebuilt artifact or a different workspace automatically.

Before adoption, qualify the exact host digest, Twenty deployment, workspace, schema, credentials, operation allowlist, webhook path, and failure topology.

Know what is excluded

The reviewed connector does not expose:

- arbitrary REST paths or HTTP methods;
- arbitrary GraphQL documents;
- API-token creation or credential material in AIP;
- file upload or attachment workflows;
- application, workflow, calendar, email, or telephony surfaces outside the fixed record and metadata catalogues;
- provider transactions or multi-operation atomicity;
- cancellation or streaming;
- provider rollback, AIP compensation, or automatic reconciliation;
- schema-specific validation of dynamic record bodies;
- compatibility with an unrecorded Twenty revision.

Choose the next path

Start with the connector catalogue for scope, then read the AIP execution model before sending Actions. Use the fleet guide for the standalone host, the error reference before implementing retries, and the upstream-baseline page when reviewing provider identity.

Related documentation

- [Connector catalog](#)
- [How AIP works](#)
- [Deploy the connector fleet](#)
- [Errors and retry decisions](#)
- [Connector upstream baselines](#)