

Environment variables

This reference lists all 86 environment variables consumed by the product-neutral getaip-server gateway and separates them from connector control-plane, standalone host, product connector, and getaip settings. Use it to identify which proce

SECTION	Deploy and Operate
TYPE	Reference
PROTOCOL	AIP 1.0
SOURCE	docs/reference/environment-variables.md

The inventory reflects source revision `d7cce13d1d555644d04a4d73c66c95b113737635`. It does not include variables used only by the migration-only bundled binary or by non-public development modules.

Choose the correct owner

Prefix	Owning process	Canonical configuration owner
<code>GETAIP_SERVER_</code>	Product-neutral getaip-server gateway	This page and 'getaip-server' configuration
<code>AIP_CONNECTOR_CONTROL_</code>	Standalone connector lifecycle control plane	Control-plane section on this page
<code>AIP_CONNECTOR_HOST_</code>	Common bootstrap for every standalone connector host	Connector host configuration
<code>AIP_CAL_DIY_</code>	Standalone Cal.diy host	Cal.diy connector-local configuration
<code>AIP_HERMES_</code>	Standalone Hermes Agent host	Hermes Agent connector-local configuration
<code>AIP_CHATWOOT_</code>	Standalone Chatwoot host	Chatwoot connector-local configuration
<code>AIP_DIFY_</code>	Standalone Dify host	Dify connector-local configuration
<code>AIP_CREWAI_</code>	Standalone CrewAI host	CrewAI connector-local configuration
<code>AIP_TWENTY_</code>	Standalone Twenty host	Twenty connector-local configuration
<code>GETAIP_</code>	getaip client process	Tool section on this page and the 'getaip' reference

Do not copy provider credentials from a standalone host into a `GETAIP_SERVER_` variable. The `AIP_CAL_DIY_` prefix is owned by the standalone Cal.diy host; it does not make Cal.diy part of the product-neutral gateway.

Resolution and parsing rules

For most scalar `getaip-server` settings, an explicit CLI value wins and the environment is the fallback. These variables are exceptions:

- `GETAIP_SERVER_NATIVE_PRINCIPAL` overrides the CLI principal, including an explicit

`--native-principal value`;

- `GETAIP_SERVER_MCP_PRINCIPAL` overrides the CLI principal, including an explicit

`--mcp-principal value`;

- `GETAIP_SERVER_NATS_REQUEST_TIMEOUT_MS` overrides

`--nats-request-timeout-ms`.

Boolean variables are true only for 1, true, TRUE, yes, or YES. Every other value, including an empty string, is false. Boolean environment and CLI switches are otherwise combined as logical OR.

Unsigned integer variables use strict decimal parsing. A malformed or negative value fails startup even when the subsystem would later remain disabled. Values that must be positive receive an additional validation check.

Two list formats exist:

Format	Separators	Variables using it
Route list	Semicolon or newline	Trusted signer and delegation specifications
General list	Comma, semicolon, or newline	Hosts, scopes, issuers, origins, topology weights, and other repeatable values

Environment list entries extend the corresponding CLI list. They do not replace it. Duplicate entries can fail a later uniqueness check.

An empty environment value is not a portable substitute for unsetting a variable. Some paths filter empty values, while other paths parse or validate them and fail. Remove an unused variable from the process environment.

getaip-server process and storage

Variable	CLI relation	Default or purpose
GETAIP_SERVER_PUBLIC_BASE_URL	Fallback for --public-base-url	External HTTPS origin advertised for A2A and discovery.
GETAIP_SERVER_STORAGE_DIR	Fallback for --storage-dir	Durable local and auxiliary file state.
GETAIP_SERVER_POSTGRES_URL	Fallback for --postgres-url	Inline clustered runtime PostgreSQL URL. Prefer the file variable.
GETAIP_SERVER_POSTGRES_URL_FILE	Fallback for --postgres-url-file	Mode-0600 file containing the runtime PostgreSQL URL.

The PostgreSQL inline and file variables are mutually exclusive after CLI and environment resolution. PostgreSQL owns core runtime state when either form resolves; otherwise the storage directory owns local runtime state. With neither, core runtime state is in memory.

The listener address, service ID, trust domain, manifest-print mode, and MCP stdio mode have no GETAIP_SERVER_ environment equivalent in this revision. Configure them with CLI options.

getaip-server native identity and authorization

Variable	Type or format	Default or purpose
GETAIP_SERVER_TRUSTED_SIGNERS	Route list of <code>DID=PRINCIPAL_ID</code>	Extends inline trusted signer bindings.
GETAIP_SERVER_TRUSTED_SIGNER_FILE	Path	Additional bounded JSON signer directory.
GETAIP_SERVER_NATIVE_BEARER_TOKEN	Secret text	Inline native HTTP bearer token. Prefer the file variable.
GETAIP_SERVER_NATIVE_BEARER_TOKEN_FILE	Secret-file path	Mode-0600 native bearer-token file.
GETAIP_SERVER_NATIVE_PRINCIPAL	Principal ID	Overrides the CLI native principal; CLI default is <code>service:getaip:server:http-edge</code> .
GETAIP_SERVER_NATIVE_TENANT_ID	Tenant ID	Verified tenant bound to native bearer authentication.
GETAIP_SERVER_NATIVE_PRINCIPAL_SCOPES	General list	Extends scopes granted to the native principal.
GETAIP_SERVER_TRUSTED_IDENTITY_FILE	Path	Revised trusted identity, tenant, credential, and context directory.
GETAIP_SERVER_APPROVAL_AUTHORITY_FILE	Path	Revised approval-authority membership directory.
GETAIP_SERVER_REQUIRE_SIGNED_ENVELOPES	Boolean	Explicitly enables signed native envelopes.
GETAIP_SERVER_ALLOW_UNSIGNED_ENVELOPES	Boolean	Disables the default signature requirement unless another require switch restores it.
GETAIP_SERVER_INSECURE_DEVELOPMENT	Boolean	Enables unauthenticated native development only on loopback.

`GETAIP_SERVER_NATIVE_BEARER_TOKEN` and `GETAIP_SERVER_NATIVE_BEARER_TOKEN_FILE` cannot both resolve. Signatures are required by default. To accept unsigned envelopes, `GETAIP_SERVER_ALLOW_UNSIGNED_ENVELOPES` must be true while the CLI and environment require switches are false. Outside loopback-only insecure development, native bearer authentication is still required for unsigned traffic.

Signer bindings from the route list and file are merged. Every signer must use a valid Ed25519 `did:key`, and a DID cannot occur twice across the combined sources.

getaip-server callbacks and runtime budgets

Variable	Type or format	Default or purpose
GETAIP_SERVER_CALLBACK_ALLOWED_HOSTS	General list	Exact outbound callback hosts.
GETAIP_SERVER_CALLBACK_SIGNING_SEED_HEX	Secret hex	Inline 32-byte response and callback signing seed. Prefer the file variable.
GETAIP_SERVER_CALLBACK_SIGNING_SEED_FILE	Secret-file path	Mode-0600 response and callback signing-seed file.
GETAIP_SERVER_A2A_PUSH_ENCRYPTION_KEY_HEX	Secret hex	Inline 32-byte key for stored A2A push credentials.
GETAIP_SERVER_CALLBACK_ALLOW_HTTP	Boolean	Permits plaintext callback and shared-policy destinations.
GETAIP_SERVER_CALLBACK_ALLOW_PRIVATE_NETWORKS	Boolean	Permits private or loopback shared-policy destinations.
GETAIP_SERVER_CALLBACK_TIMEOUT_MS	Unsigned integer	Callback request timeout; default 5000. Environment-only.
GETAIP_SERVER_CALLBACK_MAX_RESPONSE_BYTES	Unsigned integer	Callback response bound; default 4194304. Environment-only.
GETAIP_SERVER_CALLBACK_MAX_IN_FLIGHT	Positive integer	Concurrent callback deliveries; default 64.
GETAIP_SERVER_CALLBACK_RECOVERY_BATCH	Positive integer	Callback records leased per recovery cycle; default 64.
GETAIP_SERVER_RECONCILIATION_MAX_IN_FLIGHT	Positive integer	Concurrent transaction reconciliations; default 32.

The inline and file signing-seed variables are mutually exclusive. An allowed callback host, A2A push key, or delegation route requires a response and callback signing seed. The HTTP and private-network variables expand the destination boundary shared by callbacks and HTTP delegation.

getaip-server connector registry and fleet transport

Variable	Type or format	Default or purpose
GETAIP_SERVER_CONNECTOR_REGISTRY_URL	Secret text	Inline registry data-plane PostgreSQL URL. Prefer the file variable.
GETAIP_SERVER_CONNECTOR_REGISTRY_URL_FILE	Secret-file path	Mode-0600 registry data-plane URL file.
GETAIP_SERVER_CONNECTOR_REGISTRY_DATA_MAX_CONNECTIONS	Positive integer	Registry data connections; default 32.
GETAIP_SERVER_CONNECTOR_REGISTRY_ACQUIRE_TIMEOUT_MS	Positive integer	Connection wait; default 5000, maximum 60000.
GETAIP_SERVER_CONNECTOR_FLEET_SIGNING_SEED_FILE	Secret-file path	Required 32-byte Ed25519 seed file for fleet mode.
GETAIP_SERVER_CONNECTOR_FLEET_CALLBACK_URL	URL	Central stream callback ending in /aip/v1/connector-callbacks.
GETAIP_SERVER_CONNECTOR_FLEET_ALLOWED_HOSTS	General list	Exact connector-host destination hosts.
GETAIP_SERVER_CONNECTOR_FLEET_TRUST_REGISTRY_ENDPOINTS	Boolean	Uses admitted registry endpoints as the per-route host allowlist.
GETAIP_SERVER_CONNECTOR_FLEET_ALLOW_HTTP	Boolean	Permits plaintext host and fleet callback URLs.
GETAIP_SERVER_CONNECTOR_FLEET_ALLOW_PRIVATE_NETWORKS	Boolean	Permits private or loopback connector-host addresses.
GETAIP_SERVER_CONNECTOR_FLEET_TIMEOUT_MS	Positive integer	Connector-host request timeout; default 5000.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_RESPONSE_BYTES	Positive integer	Host response bound; default 4194304.
GETAIP_SERVER_CONNECTOR_FLEET_RETRY_BUDGET	Unsigned integer	Retries after the first attempt; default 2.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_CACHED_CLIENTS	Positive integer	Cached host HTTP pools; default 256.
GETAIP_SERVER_CONNECTOR_FLEET_TLS_CA_FILE	Path	Additional PEM root for private-PKI host TLS.

The registry inline and file variables are mutually exclusive. A resolved registry URL activates fleet composition and then requires the signing-seed file plus either explicit allowed hosts or registry endpoint trust.

getaip-server fleet topology and admission

Variable	Type or format	Default or purpose
GETAIP_SERVER_CONNECTOR_FLEET_REGION	Text	Preferred region for new assignments; unset by default.
GETAIP_SERVER_CONNECTOR_FLEET_ZONE	Text	Preferred zone for new assignments; unset by default.
GETAIP_SERVER_CONNECTOR_FLEET_CAPACITY_CLASS	Text	Required capacity class for new assignments; unset by default.
GETAIP_SERVER_CONNECTOR_FLEET_DISABLE_CROSS_REGION_FAILOVER	Boolean	Forbids new-assignment fallback to another region.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_IN_FLIGHT	Positive integer	Global active remote actions; default 1024.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_IN_FLIGHT_PER_TENANT	Positive integer	Active remote actions per tenant; default 128.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_QUEUED	Positive integer	Global waiting actions; default 4096.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_QUEUED_PER_TENANT	Positive integer	Waiting actions per tenant; default 512.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_QUEUED_BYTES	Positive integer	Canonical bytes retained by queued actions; default 67108864.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_REQUEST_BYTES	Positive integer	Canonical size of one remote action; default 4194304.
GETAIP_SERVER_CONNECTOR_FLEET_MAX_QUEUED_AGE_MS	Positive integer	Maximum local queue time; default 30000.
GETAIP_SERVER_CONNECTOR_FLEET_TENANT_WEIGHTS	General list of TENANT_ID=WEIGHT	Positive scheduling weights; none by default.

Per-tenant limits cannot exceed their global counterparts. Weight tenant IDs contain 1–256 bytes, each weight is positive, and duplicate tenant IDs fail startup. Topology preferences affect new assignments, not already pinned work.

getaip-server fleet activation nuance

GETAIP_SERVER_CONNECTOR_REGISTRY_URL or GETAIP_SERVER_CONNECTOR_REGISTRY_URL_FILE is the only environment activation boundary for fleet mode. Do not infer activation from another fleet variable.

Without a registry URL, these environment groups explicitly make the configuration partial and fail startup:

- signing-seed file and fleet callback URL;
- allowed hosts or any fleet network-policy Boolean;
- tenant weights;
- cross-region failover disablement;
- any connector-event or stream-ingress limit.

Valid environment-only pool, transport numeric, topology text, admission numeric, and TLS CA settings do not activate fleet mode and are not all treated as partial configuration in the reviewed implementation. They can be parsed or their file can be read, then discarded when the registry URL is absent. An invalid numeric value or unreadable CA file can still fail startup.

Set the registry URL explicitly and verify the `/ready` fleet section rather than using a tuning value as an activation probe.

getaip-server connector-event and stream ingress

Variable	Type	Default or purpose
GETAIP_SERVER_CONNECTOR_EVENT_MAX_ENVELOPE_BYTES	Positive integer	Signed envelope bound; default 4194304.
GETAIP_SERVER_CONNECTOR_EVENT_MAX_EVENTS_PER_ENVELOPE	Integer 1-1000	Events per envelope; default 100.
GETAIP_SERVER_CONNECTOR_EVENT_MAX_EVENT_BYTES	Positive integer	One enriched event; default 262144, no more than envelope bound.
GETAIP_SERVER_CONNECTOR_STREAM_MAX_CHUNK_BYTES	Positive integer	One stream chunk; default 262144, no more than envelope bound.
GETAIP_SERVER_CONNECTOR_EVENT_MAX_INFLIGHT	Positive integer	Concurrent storage operations; default 128.
GETAIP_SERVER_CONNECTOR_EVENT_MAX_AGE_SECONDS	Positive integer	Maximum event age; default 86400.
GETAIP_SERVER_CONNECTOR_EVENT_MAX_FUTURE_SKEW_SECONDS	Positive integer	Future clock skew; default 300.
GETAIP_SERVER_CONNECTOR_STREAM_CALLBACK_MAX_AGE_SECONDS	Positive integer	Signed stream callback age; default 300.

Any one of these variables without a registry URL is rejected as partial fleet configuration. The limits do not replace route, tenant, signature, timestamp, sequence, lease, or replay validation.

getaip-server NATS and delegation

Variable	Type or format	Default or purpose
GETAIP_SERVER_NATS_URL	URL	Enables native NATS request/reply.
GETAIP_SERVER_NATS_USERNAME	Text	NATS username; requires the password file.
GETAIP_SERVER_NATS_PASSWORD_FILE	Secret-file path	Mode-0600 NATS password; requires the username.
GETAIP_SERVER_NATS_TRUST_DOMAIN	Text	Subject trust domain; defaults to the daemon trust domain.
GETAIP_SERVER_NATS_SERVICE	Text	Subject service; default <code>getaip-server</code> .
GETAIP_SERVER_NATS_VERSION	Text	Subject version; default <code>v1</code> .
GETAIP_SERVER_NATS_QUEUE_GROUP	Text	Optional queue group.
GETAIP_SERVER_NATS_REQUEST_TIMEOUT_MS	Unsigned integer	Request timeout; overrides CLI, whose default is 30000.
GETAIP_SERVER_DELEGATION_HTTP_ROUTES	Route list	DELEGATE_ID=URL, PEER_ID, PEER_DID[, TRUST_DOMAIN].
GETAIP_SERVER_DELEGATION_NATS_ROUTES	Route list	CAPABILITY_ID=SERVER_URL, SUBJECT, PEER_ID, PEER_DID[, TIMEOUT_MS[, TRUST_DOMAIN]].

Authentication values without `GETAIP_SERVER_NATS_URL` fail startup. Username and password file must resolve together. Delegation lists extend CLI routes and require the response and callback signing seed.

getaip-server MCP

Variable	Type or format	Default or purpose
GETAIP_SERVER_MCP_BEARER_TOKEN	Secret text	Static MCP HTTP bearer token.
GETAIP_SERVER_MCP_RESOURCE	Resource identifier	Protected-resource identifier.
GETAIP_SERVER_MCP_AUTHORIZATION_SERVERS	General list	Advertised authorization-server issuers.
GETAIP_SERVER_MCP_SCOPES	General list	Advertised supported scopes.
GETAIP_SERVER_MCP_REQUIRED_SCOPES	General list	Scopes required to establish an MCP HTTP session.
GETAIP_SERVER_MCP_RESOURCE_DOCUMENTATION	URL	Human-readable protected-resource documentation.
GETAIP_SERVER_MCP_ALLOWED_ORIGINS	General list	Browser origins allowed to call MCP HTTP.
GETAIP_SERVER_MCP_INTROSPECTION_URL	HTTPS URL	RFC 7662 endpoint.
GETAIP_SERVER_MCP_INTROSPECTION_ISSUER	Issuer	Trusted issuer represented by introspection.
GETAIP_SERVER_MCP_INTROSPECTION_CLIENT_ID	Text	OAuth introspection client ID.
GETAIP_SERVER_MCP_INTROSPECTION_CLIENT_SECRET_FILE	Secret-file path	Mode-0600 introspection client secret.
GETAIP_SERVER_MCP_INTROSPECTION_ALLOW_LOOPBACK_HTTP	Boolean	Permits a loopback plaintext introspection fixture.
GETAIP_SERVER_MCP_PRINCIPAL	Principal ID	Overrides the CLI MCP principal; CLI default is <code>service:getaip:server:mcp-edge</code> .
GETAIP_SERVER_MCP_PRINCIPAL_SCOPES	General list	Extends scopes granted to the MCP principal.

Introspection URL, issuer, client ID, and secret file are an all-or-none group. Introspection also requires a protected resource, rejects a simultaneous static token, and requires its issuer in the advertised authorization-server list.

When resource is absent, a static token, authorization server, supported scope, or documentation URL causes the implementation to derive `http://mcp`. Set `GETAIP_SERVER_MCP_RESOURCE` explicitly for a public origin.

Connector control-plane variables

The standalone `aip-connector-control-plane` consumes two environment variables:

Variable	CLI relation	Purpose
AIP_CONNECTOR_CONTROL_DATABASE_URL_FILE	Fallback for <code>--database-url-file</code>	Required owner-only file containing the restricted lifecycle PostgreSQL URL.
AIP_CONNECTOR_CONTROL_SIGNING_SEED_FILE	Fallback for <code>--signing-seed-file</code>	Required owner-only file containing the response-signing Ed25519 seed.

An explicit CLI path wins. Empty environment paths are treated as absent. Both files must be regular non-symlink files with no group or other permission bits. Other control-plane settings, including bind address, proxy-network exception, principal ID, lease TTL, pool size, and acquire timeout, are CLI-only in this revision.

Standalone connector-host variables

Every one of the six public standalone hosts consumes the 45 common `AIP_CONNECTOR_HOST_` variables documented in the Connector host configuration page linked from the ownership table. That page is the canonical inventory for common endpoint, admitted identity, tenant, trust, storage, topology, credential, lifecycle, callback, event, and limit settings.

Each host then adds its product-owned prefix shown in the ownership table. The connector-local configuration page owns those provider endpoints, account or workspace identifiers, operation descriptors, policy files, and credential

file references. This global page does not duplicate them because their required combinations and defaults differ by connector.

getaip variables

Variable	Default or purpose
GETAIP_NATIVE_BEARER_TOKEN	Fallback inline native HTTP bearer token. Prefer the file variable.
GETAIP_NATIVE_BEARER_TOKEN_FILE	Owner-only native bearer-token file.
GETAIP_NATIVE_SIGNING_SEED_FILE	Owner-only Ed25519 seed file for signed native HTTP requests.
GETAIP_NATIVE_PRINCIPAL_ID	Signed native principal; environment overrides CLI, whose default is <code>agent:getaip:cli</code> .
GETAIP_NATIVE_TRUST_DOMAIN	Trust domain carried by signed native HTTP requests.
GETAIP_NATIVE_TLS_CA_FILE	Additional PEM root for native private-PKI TLS.
GETAIP_NATIVE_PEER_DID	Pinned Ed25519 DID expected on native responses.
GETAIP_NATIVE_PEER_DID_FILE	File containing the pinned response DID; mutually exclusive with inline DID.
GETAIP_NATIVE_MAX_RESPONSE_BYTES	Native HTTP response bound; environment overrides CLI, whose default is <code>4194304</code> .
GETAIP_NATS_USERNAME	Native NATS username; requires the password file.
GETAIP_NATS_PASSWORD_FILE	Owner-only native NATS password file; requires the username.
GETAIP_NATS_SIGNING_SEED_FILE	Owner-only Ed25519 seed file for signed native NATS requests.
GETAIP_MCP_BEARER_TOKEN	Fallback bearer token for MCP HTTP subcommands.

Except for the documented principal and response-size overrides, explicit `getaip` options take precedence. Do not export long-lived inline tokens into a shared shell profile. Prefer owner-only files and give the CLI process access only for the duration of the operation.

The native bearer token and bearer-token file are mutually exclusive. The inline native peer DID and peer-DID file are also mutually exclusive. NATS username and password file must resolve together; the NATS signing seed remains a separate AIP message-signing identity.