



MHI Gateway

API Reference

SMS API v1

Contract version 1.0.0-rc1

Document version 1.0

Publication date 28 July 2026

Classification Public API documentation

MICRO HEALTH INITIATIVE

Document Control

Field	Value
Document title	MHI Gateway API Reference
Document identifier	MHI-SMS-API-REFERENCE-V1
Contract version	1.0.0-rc1
Document version	1.0
Status	Milestone 2
Audience	API consumers, solution architects, and integration engineers
Authoritative specification	docs/api/openapi.yaml
Companion guide	Developer Integration Guide

This reference describes the frozen public SMS API contract. If this document and OpenAPI differ, OpenAPI governs. The companion [Developer Integration Guide](#) explains integration patterns, operational practices, and production readiness.

Revision History

Version	Date	Status	Description
1.0	28 July 2026	Initial	Official API Reference for contract 1.0.0-rc1

Table of Contents

Document Control	2
Revision History	2
Table of Contents	3
1 Overview	8
1.1 Base URL	8
1.2 Public operations	8
1.3 Media type and encoding	8
1.4 Contract boundaries	8
2 Authentication Summary	9
3 Common Headers	10
3.1 API request headers	10
3.2 API response headers	10
3.3 Outbound webhook request headers	10
4 Standard Response Format	11
4.1 Single-message acceptance	11
4.2 Bulk result	11
4.3 Resource timestamps	11
5 Error Response Format	12
6 Rate Limiting	13
7 Correlation IDs	14
8 Idempotency	15
9 Endpoint Reference	16
9.1 Submit one SMS message	16
Purpose	16
HTTP method and URL	16
Authentication	16
Headers	16
Path parameters	16
Query parameters	16
Request body	16
Request example	16
Success response	16
Response headers	17
Response body	17

Possible errors	17
HTTP status codes	17
Notes	17
Best practices	17
Related endpoints	17
9.2 Submit a bulk SMS request	17
Purpose	17
HTTP method and URL	17
Authentication	17
Headers	18
Path parameters	18
Query parameters	18
Request body	18
Request example	18
Success response	18
Response headers	19
Response body	19
Possible errors	19
HTTP status codes	19
Notes	19
Best practices	19
Related endpoints	19
9.3 Retrieve one message	19
Purpose	19
HTTP method and URL	19
Authentication	19
Headers	20
Path parameters	20
Query parameters	20
Request body	20
Validation rules	20
Request example	20
Success response	20
Response headers	20
Response body	20
Possible errors	21
HTTP status codes	21
Notes	21
Best practices	21
Related endpoints	21
9.4 Retrieve normalized message status	21
Purpose	21
HTTP method and URL	21
Authentication	21
Headers	21

Path parameters	21
Query parameters	21
Request body	21
Validation rules	22
Request example	22
Success response	22
Response headers	22
Response body	22
Possible errors	22
HTTP status codes	22
Notes	22
Best practices	22
Related endpoints	22
9.5 Replace delivery webhook configuration	22
Purpose	22
HTTP method and URL	23
Authentication	23
Headers	23
Path parameters	23
Query parameters	23
Request body	23
Request example	23
Success response	23
Response headers	24
Response body	24
Possible errors	24
HTTP status codes	24
Notes	24
Best practices	24
Related endpoints	24
9.6 Retrieve delivery webhook configuration	24
Purpose	24
HTTP method and URL	24
Authentication	24
Headers	24
Path parameters	25
Query parameters	25
Request body	25
Validation rules	25
Request example	25
Success response	25
Response headers	25
Response body	25
Possible errors	25
HTTP status codes	25

Notes	25
Best practices	25
Related endpoints	26
9.7 Webhook callback reference	26
9.7.1 Configuration	26
9.7.2 Delivery status webhook	26
10 Common Schemas	28
10.1 CorrelationId	28
10.2 MessageId	28
10.3 MessageStatus	28
10.4 Timestamp	28
10.5 MessageSubmission	28
10.6 MessageAccepted	28
10.7 MessageDetails	29
10.8 MessageStatusResource	29
10.9 BatchId	29
10.10 BulkSubmission	29
10.11 BulkMessageCandidate	30
10.12 BulkAcceptedResult	30
10.13 BulkRejectedResult	30
10.14 BulkItemError	30
10.15 BulkItemResult	30
10.16 BulkResult	31
10.17 DeliveryWebhookWrite	31
10.18 DeliveryWebhookRead	31
10.19 DeliveryWebhookEvent	31
10.20 ErrorBody	31
10.21 ErrorResponse	32
11 Response Headers	33
11.1 API responses	33
11.2 Idempotent replay	33
11.3 Webhook acknowledgment	33
12 Error Codes	34
12.1 Request-level errors	34
12.2 Bulk item errors	34
13 Status Values	35
13.1 Public message statuses	35
13.2 Allowed transitions	35
13.3 Webhook statuses	35
14 Appendices	36

Appendix A: Endpoint matrix 36

Appendix B: Reusable parameters 36

Appendix C: Reusable OpenAPI responses 36

Appendix D: Identifier formats 36

Appendix E: Source precedence and route inventory 37

Appendix F: Related resources 37

1 Overview

MHI Gateway exposes a tenant-scoped REST API for submitting SMS messages, retrieving normalized message resources, and managing one delivery webhook configuration. API requests and responses use UTF-8 JSON over HTTPS in production.

1.1 Base URL

The OpenAPI server path is:

```
/api/v1
```

Combine the path with the environment host supplied by the gateway operator:

```
https://<API_HOST>/api/v1
```

1.2 Public operations

Operation ID	Method	Path	Success
submitMessage	POST	/messages	202
submitMessageBulk	POST	/messages/bulk	202
getMessage	GET	/messages/{message_id}	200
getMessageStatus	GET	/messages/{message_id}/status	200
replaceDeliveryWebhook	PUT	/webhook	200
getDeliveryWebhook	GET	/webhook	200

All paths in this reference are relative to /api/v1 unless shown as complete URLs. The API also defines one outbound [delivery webhook](#) sent by MHI Gateway.

1.3 Media type and encoding

Request bodies and response bodies use:

```
Content-Type: application/json
```

JSON strings are UTF-8. Object schemas with `additionalProperties: false` reject fields that are not declared by the contract.

1.4 Contract boundaries

The contract does not define a public batch resource, batch retrieval, cancellation, scheduled messages, templates, campaigns, multiple webhook endpoints, webhook deletion, event filtering, or webhook retry scheduling.

2 Authentication Summary

Every API operation requires HTTP Bearer authentication:

```
Authorization: Bearer <API_TOKEN>
```

The implemented credential format is:

```
mhi_<environment>_<12-character-prefix>.<48-character-secret>
```

The credential resolves to one active tenant and application. Treat it as an opaque secret. An absent or invalid credential returns **401** using the standard error envelope with **AUTHENTICATION_FAILED**.

Authorization and tenant-isolation guidance is in the [Developer Integration Guide](#).

3 Common Headers

3.1 API request headers

Header	Required	Applies to	Value and constraints
Authorization	Yes	Every API request	Bearer <API_TOKEN>
Accept	Recommended	Every API request	application/json
Content-Type	Yes when a JSON body is sent	POST and PUT requests	application/json
Idempotency-Key	Yes	Both submission operations	Visible ASCII, 1-191 characters
X-Correlation-ID	No	Every API request	1-100 characters matching [A-Za-z0-9][A-Za-z0-9._:-]{0,99}

X-Request-ID is a response header; it is not a client request parameter in the approved contract.

3.2 API response headers

Every HTTP response, successful or unsuccessful, carries:

Header	Required	Meaning
X-Request-ID	Yes	Unique identifier for the current HTTP request
X-Correlation-ID	Yes	Current request correlation identifier

Successful JSON responses also carry Content-Type: application/json.

3.3 Outbound webhook request headers

Header	Required	Value and constraints
Content-Type	Yes	application/json
X-Webhook-Timestamp	Yes	Unix seconds, integer int64
X-Webhook-Signature	Yes	v1= followed by 64 lowercase hexadecimal characters

The signature is HMAC-SHA256 over <timestamp>.<raw-request-body> using the configured secret.

4 Standard Response Format

Successful responses are JSON objects. The API does not add a common wrapper around successful resources.

4.1 Single-message acceptance

```
{
  "message_id": "01JEXAMPLE0000000000000000",
  "status": "queued",
  "client_reference": "order-1042",
  "created_at": "2026-07-19T12:30:40.123456Z",
  "correlation_id": "order-1042-attempt-1"
}
```

4.2 Bulk result

```
{
  "batch_id": "550e8400-e29b-41d4-a716-446655440001",
  "accepted": 1,
  "rejected": 1,
  "results": [
    {
      "index": 0,
      "message_id": "01JEXAMPLE0000000000000000",
      "status": "queued"
    },
    {
      "index": 1,
      "error": {
        "code": "INVALID_RECIPIENT",
        "message": "Recipient is invalid.",
        "details": {}
      }
    }
  ]
}
```

4.3 Resource timestamps

API resource timestamps use UTC RFC 3339. Persisted resources retain microseconds.

5 Error Response Format

Request-level errors use ErrorResponse:

```
{
  "error": {
    "code": "INVALID_REQUEST",
    "message": "The request is invalid.",
    "details": {},
    "correlation_id": "01JEXAMPLE0000000000000000"
  }
}
```

Property	Type	Required	Description
error	ErrorBody	Yes	Error object
error.code	string	Yes	Stable official error code
error.message	string	Yes	Sanitized human-readable message
error.details	object	Yes	Safe structured details; may be empty
error.correlation_id	string	Yes	Current request correlation identifier

Bulk item errors use BulkItemError, not the request-level envelope. See [BulkItemError](#).

6 Rate Limiting

Every operation may return:

`HTTP/1.1 429 Too Many Requests`

The response uses the standard error envelope and the official `RATE_LIMIT_EXCEEDED` code. The approved contract does not specify public quotas, rate windows, or an additional rate-limit response-header schema. Consumers must not depend on undocumented limit values.

The route inventory applies separate read and write throttle middleware, but their numeric policies are not part of the public API contract.

7 Correlation IDs

The API exposes three distinct identifier roles:

Identifier	Location	Meaning
X-Request-ID	Every response header	Unique identifier for the current HTTP request
X-Correlation-ID	Optional request header and every response header	Current request correlation identifier; a valid client value is preserved, otherwise the gateway generates a UUIDv4
correlation_id	Resource or error body	Correlation value defined by that response schema

For `MessageAccepted`, body `correlation_id` is the original submission correlation identifier. It remains unchanged on idempotent replay. The response headers identify the current replay request.

For message retrieval resources and error bodies, `correlation_id` is the current request correlation identifier.

Capture `X-Request-ID` and `X-Correlation-ID` from successful and error responses.

8 Idempotency

The two submission endpoints require Idempotency-Key.

Rule	Contract
Scope	Tenant
Length	1-191 characters
Character set	Visible ASCII
First valid request	Durably binds the key to canonical input and the original result
Equivalent replay	Returns the original result and status code
Different canonical input	Returns 409 IDEMPOTENCY_CONFLICT
Failed validation	Does not bind the key
Bulk ordering	Array order is part of canonical equivalence

For bulk submissions, equivalent replay retains the original `batch_id`, counters, ordered item results, and item identities. `batch_id` is not a replacement for `X-Correlation-ID`.

Idempotency retention remains unresolved in the frozen contract. No retention duration is stated by this reference.

9 Endpoint Reference

9.1 Submit one SMS message

Purpose

Accept one SMS message for asynchronous processing.

HTTP method and URL

```
POST /api/v1/messages
```

Operation ID: submitMessage

Authentication

Bearer authentication is required.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
Content-Type	Yes	application/json
Idempotency-Key	Yes	Visible ASCII, 1-191 characters
X-Correlation-ID	No	Valid CorrelationId

Path parameters

None.

Query parameters

None.

Request body

Schema: [MessageSubmission](#)

Property	Type	Required	Validation
recipient	string	Yes	E.164 pattern <code>^\+[1-9][0-9]{7,14}\$</code>
message	string	Yes	1-4096 characters
sender_id	string	Yes	1-11 ASCII alphanumeric; active assignment
client_reference	string	No	1-100 characters; restricted correlation pattern

Unknown fields are rejected. sender_id is required and must be active and assigned to the authenticated application.

Request example

```
curl --request POST 'https://<API_HOST>/api/v1/messages' \
  --header 'Authorization: Bearer <API_TOKEN>' \
  --header 'Accept: application/json' \
  --header 'Content-Type: application/json' \
  --header 'Idempotency-Key: 6b11f086-1e8d-4bb9-a680-1524e8d23b21' \
  --header 'X-Correlation-ID: order-1042-attempt-1' \
  --data '{
    "recipient": "+255712345678",
    "message": "Your verification code is 123456.",
    "sender_id": "MHI",
    "client_reference": "order-1042"
  }'
```

Success response

```
HTTP/1.1 202 Accepted
Content-Type: application/json
X-Request-ID: 01JREQUEST000000000000000000
X-Correlation-ID: order-1042-attempt-1
```

Schema: [MessageAccepted](#)

```
{
  "message_id": "01JEXAMPLE0000000000000000",
  "status": "queued",
  "client_reference": "order-1042",
  "created_at": "2026-07-19T12:30:40.123456Z",
  "correlation_id": "order-1042-attempt-1"
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

`message_id`, `status`, `created_at`, and `correlation_id` are required. `client_reference` is optional.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
409	IdempotencyConflict	Key is bound to different canonical input
422	ValidationError	Request validation failed
429	RateLimited	Rate limit exceeded
500	InternalServerError	Sanitized internal failure

HTTP status codes

202, 401, 409, 422, 429, 500.

Notes

202 indicates acceptance, not delivery. On equivalent replay, the body is the original result; X-Request-ID and X-Correlation-ID describe the current request.

Best practices

Persist the idempotency key, complete original response, and `message_id`.

Related endpoints

- [Retrieve one message](#)
- [Retrieve normalized message status](#)

9.2 Submit a bulk SMS request

Purpose

Evaluate an ordered collection of 1-100 SMS candidates using best-effort, partial-success processing.

HTTP method and URL

```
POST /api/v1/messages/bulk
```

Operation ID: `submitMessageBulk`

Authentication

Bearer authentication is required.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
Content-Type	Yes	application/json
Idempotency-Key	Yes	Visible ASCII, 1-191 characters
X-Correlation-ID	No	Valid CorrelationId

Path parameters

None.

Query parameters

None.

Request body

Schema: [BulkSubmission](#)

Property	Type	Required	Validation
client_reference	string	No	1-100 characters; restricted correlation pattern
messages	array of BulkMessageCandidate	Yes	1-100 ordered items

The top-level object and each candidate reject unknown properties. Candidate fields are independently evaluated after top-level acceptance.

Request example

```
curl --request POST 'https://<API_HOST>/api/v1/messages/bulk' \  
  --header 'Authorization: Bearer <API_TOKEN>' \  
  --header 'Accept: application/json' \  
  --header 'Content-Type: application/json' \  
  --header 'Idempotency-Key: 991f43da-8677-4b7b-8127-c4e8f5d989e3' \  
  --header 'X-Correlation-ID: campaign-42-attempt-1' \  
  --data '{  
    "client_reference": "campaign-42",  
    "messages": [  
      {  
        "recipient": "+255712345678",  
        "message": "Your appointment is confirmed.",  
        "sender_id": "MHI",  
        "client_reference": "row-1"  
      },  
      {  
        "recipient": "invalid",  
        "message": "Your appointment is confirmed.",  
        "client_reference": "row-2"  
      }  
    ]  
  }'
```

Success response

```
HTTP/1.1 202 Accepted  
Content-Type: application/json  
X-Request-ID: 01JREQUEST000000000000000001  
X-Correlation-ID: campaign-42-attempt-1
```

Schema: [BulkResult](#)

```
{  
  "batch_id": "550e8400-e29b-41d4-a716-446655440001",  
  "client_reference": "campaign-42",  
  "accepted": 1,  
  "rejected": 1,  
  "results": [  
    {  
      "index": 0,  
      "message_id": "01JEXAMPLE0000000000000000",  
      "status": "queued",  
      "client_reference": "row-1"  
    },  
    {  
      "index": 1,  
      "message_id": "01JEXAMPLE0000000000000000",  
      "status": "failed",  
      "client_reference": "row-2"  
    }  
  ]  
}
```

```
{
  "index": 1,
  "error": {
    "code": "INVALID_RECIPIENT",
    "message": "Recipient is invalid.",
    "details": {}
  }
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

batch_id, accepted, rejected, and results are required. Every input item has exactly one result with the same zero-based index.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
409	IdempotencyConflict	Key is bound to different canonical input
422	ValidationError	Top-level request validation failed
429	RateLimited	Rate limit exceeded
500	InternalServerError	Failure occurred before a stable result existed

HTTP status codes

202, 401, 409, 422, 429, 500.

Notes

A valid evaluated request returns 202 even when every item is rejected. batch_id is replay-stable tracking metadata and is not a public resource.

Best practices

Process results by index; persist each accepted message_id and the original ordered result.

Related endpoints

- [Submit one SMS message](#)
- [Retrieve normalized message status](#)

9.3 Retrieve one message

Purpose

Return the approved full public representation of one message in the authenticated scope.

HTTP method and URL

```
GET /api/v1/messages/{message_id}
```

Operation ID: getMessage

Authentication

Bearer authentication is required.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
X-Correlation-ID	No	Valid CorrelationId

Path parameters

Parameter	Type	Required	Validation
message_id	string	Yes	26 characters matching [0-9A-HJKMNP-TV-Z]{26}

Query parameters

None.

Request body

None.

Validation rules

message_id must satisfy the MessageId schema. Resource lookup remains tenant- and application-scoped.

Request example

```
curl 'https://<API_HOST>/api/v1/messages/01JEXAMPLE0000000000000000' \  
  --header 'Authorization: Bearer <API_TOKEN>' \  
  --header 'Accept: application/json' \  
  --header 'X-Correlation-ID: message-read-1042'
```

Success response

```
HTTP/1.1 200 OK  
Content-Type: application/json  
X-Request-ID: 01JREQUEST000000000000000002  
X-Correlation-ID: message-read-1042
```

Schema: [MessageDetails](#)

```
{  
  "message_id": "01JEXAMPLE0000000000000000",  
  "recipient": "+255712345678",  
  "sender_id": "MHI",  
  "client_reference": "order-1042",  
  "status": "submitted",  
  "created_at": "2026-07-19T12:30:40.123456Z",  
  "submitted_at": "2026-07-19T12:30:41.234567Z",  
  "correlation_id": "message-read-1042"  
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

message_id, recipient, status, created_at, and correlation_id are required. sender_id, client_reference, submitted_at, and finalized_at are optional.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
404	NotFound	Resource is absent from the authenticated scope
429	RateLimited	Rate limit exceeded
500	InternalServerError	Sanitized internal failure

HTTP status codes

200, 401, 404, 429, 500.

Notes

Cross-scope absence does not disclose resource existence. Message content, provider identifiers, internal IDs, and provider evidence are not returned by this schema.

Best practices

Use this operation when the complete approved resource is required. Use the compact status operation for routine reconciliation.

Related endpoints

- [Retrieve normalized message status](#)
- [Submit one SMS message](#)

9.4 Retrieve normalized message status

Purpose

Return the compact normalized status resource for one message.

HTTP method and URL

```
GET /api/v1/messages/{message_id}/status
```

Operation ID: getMessageStatus

Authentication

Bearer authentication is required.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
X-Correlation-ID	No	Valid CorrelationId

Path parameters

Parameter	Type	Required	Validation
message_id	string	Yes	26 characters matching [0-9A-HJKMNP-TV-Z]{26}

Query parameters

None.

Request body

None.

Validation rules

message_id must satisfy the MessageId schema. Resource lookup remains tenant- and application-scoped.

Request example

```
curl 'https://<API_HOST>/api/v1/messages/01JEXAMPLE00000000000000/status' \  
  --header 'Authorization: Bearer <API_TOKEN>' \  
  --header 'Accept: application/json' \  
  --header 'X-Correlation-ID: status-read-1042'
```

Success response

```
HTTP/1.1 200 OK  
Content-Type: application/json  
X-Request-ID: 01JREQUEST000000000000000003  
X-Correlation-ID: status-read-1042
```

Schema: [MessageStatusResource](#)

```
{  
  "message_id": "01JEXAMPLE0000000000000000",  
  "status": "delivered",  
  "occurred_at": "2026-07-19T12:30:44.987654Z",  
  "client_reference": "order-1042",  
  "correlation_id": "status-read-1042"  
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

message_id, status, occurred_at, and correlation_id are required. client_reference is optional.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
404	NotFound	Resource is absent from the authenticated scope
429	RateLimited	Rate limit exceeded
500	InternalServerError	Sanitized internal failure

HTTP status codes

200, 401, 404, 429, 500.

Notes

This operation deliberately omits message content. occurred_at is the authoritative transition time represented by the resource.

Best practices

Use this operation to reconcile messages that remain queued, submitted, or unknown.

Related endpoints

- [Retrieve one message](#)
- [Delivery status webhook](#)

9.5 Replace delivery webhook configuration

Purpose

Create the tenant's single delivery webhook configuration when absent or completely replace it when present.

HTTP method and URL

```
PUT /api/v1/webhook
```

Operation ID: `replaceDeliveryWebhook`

Authentication

Bearer authentication is required. The authenticated principal must be permitted to manage the configuration.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
Content-Type	Yes	application/json
X-Correlation-ID	No	Valid CorrelationId

Path parameters

None.

Query parameters

None.

Request body

Schema: [DeliveryWebhookWrite](#)

Property	Type	Required	Validation
url	string	Yes	URI; HTTPS is mandatory in production
secret	string	Yes	At least 32 cryptographically random bytes; write-only
enabled	boolean	Yes	true or false

Unknown fields are rejected.

Request example

```
curl --request PUT 'https://<API_HOST>/api/v1/webhook' \  
  --header 'Authorization: Bearer <API_TOKEN>' \  
  --header 'Accept: application/json' \  
  --header 'Content-Type: application/json' \  
  --header 'X-Correlation-ID: webhook-config-1' \  
  --data '{  
    "url": "https://example.com/webhooks/mhi-gateway",  
    "secret": "<AT_LEAST_32_RANDOM_BYTES>",  
    "enabled": true  
  }'
```

Success response

```
HTTP/1.1 200 OK  
Content-Type: application/json  
X-Request-ID: 01JREQUEST0000000000000004  
X-Correlation-ID: webhook-config-1
```

Schema: [DeliveryWebhookRead](#)

```
{  
  "url": "https://example.com/webhooks/mhi-gateway",  
  "enabled": true,  
  "created_at": "2026-07-19T12:00:00.000000Z",  
  "updated_at": "2026-07-19T12:00:00.000000Z"  
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

url, enabled, created_at, and updated_at are required. The secret is never returned.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
403	Forbidden	Principal is not permitted
422	ValidationError	Configuration validation failed
429	RateLimited	Rate limit exceeded
500	InternalServerError	Sanitized internal failure

HTTP status codes

200, 401, 403, 422, 429, 500.

Notes

The newest secret becomes active immediately. The previous secret remains valid for receiver verification for 24 hours. There is no separate rotation endpoint.

Best practices

Generate the secret using a cryptographically secure source and retain the previous secret for the defined overlap when replacing a configuration.

Related endpoints

- [Retrieve delivery webhook configuration](#)
- [Delivery status webhook](#)

9.6 Retrieve delivery webhook configuration

Purpose

Return the safe representation of the tenant's delivery webhook configuration.

HTTP method and URL

```
GET /api/v1/webhook
```

Operation ID: getDeliveryWebhook

Authentication

Bearer authentication is required. The authenticated principal must be permitted to read the configuration.

Headers

Header	Required	Value
Authorization	Yes	Bearer <API_TOKEN>
Accept	Recommended	application/json
X-Correlation-ID	No	Valid CorrelationId

Path parameters

None.

Query parameters

None.

Request body

None.

Validation rules

No path, query, or body parameters are defined.

Request example

```
curl 'https://<API_HOST>/api/v1/webhook' \  
  --header 'Authorization: Bearer <API_TOKEN>' \  
  --header 'Accept: application/json' \  
  --header 'X-Correlation-ID: webhook-read-1'
```

Success response

```
HTTP/1.1 200 OK  
Content-Type: application/json  
X-Request-ID: 01JREQUEST0000000000000005  
X-Correlation-ID: webhook-read-1
```

Schema: [DeliveryWebhookRead](#)

```
{  
  "url": "https://example.com/webhooks/mhi-gateway",  
  "enabled": true,  
  "created_at": "2026-07-19T12:00:00.000000Z",  
  "updated_at": "2026-07-19T12:00:00.000000Z"  
}
```

Response headers

Header	Required	Description
X-Request-ID	Yes	Unique identifier for this HTTP request
X-Correlation-ID	Yes	Correlation identifier for this HTTP request

Response body

url, enabled, created_at, and updated_at are required. The secret is write-only and never appears.

Possible errors

HTTP status	Response	Meaning
401	AuthenticationFailed	Credential is absent or invalid
403	Forbidden	Principal is not permitted
404	NotFound	Configuration is absent from the authenticated scope
429	RateLimited	Rate limit exceeded
500	InternalServerError	Sanitized internal failure

HTTP status codes

200, 401, 403, 404, 429, 500.

Notes

The response never exposes the current or previous secret.

Best practices

Use the returned timestamps and enabled value to confirm the intended configuration without attempting to recover the secret.

Related endpoints

- [Replace delivery webhook configuration](#)
- [Delivery status webhook](#)

9.7 Webhook callback reference

9.7.1 Configuration

Configure the callback using [Replace delivery webhook configuration](#). The contract supports exactly one delivery webhook per tenant.

9.7.2 Delivery status webhook

Purpose

Notify the configured receiver when a message first reaches a terminal public status.

HTTP method and URL

POST <CONFIGURED_WEBHOOK_URL>

The URL is supplied by the tenant and is not an MHI Gateway API path.

Authentication

Bearer authentication is not used. Authenticity is established with the HMAC-SHA256 signature headers.

Headers

Header	Required	Validation
Content-Type	Yes	application/json
X-Webhook-Timestamp	Yes	Unix seconds, integer int64
X-Webhook-Signature	Yes	Pattern ^v1=[0-9a-f]{64}\$

Path parameters

Defined by the receiver URL, not by this contract.

Query parameters

None are defined by this contract.

Request body

Schema: [DeliveryWebhookEvent](#)

Property	Type	Required	Validation
message_id	string	Yes	MessageId
status	string	Yes	delivered, failed, expired, or rejected
client_reference	string	No	Client metadata
delivered_at	string	No	UTC RFC 3339 date-time
timestamp	string	Yes	UTC RFC 3339 date-time

Unknown fields are not part of the approved payload.

Request example

```
POST /webhooks/mhi-gateway HTTP/1.1
Host: example.com
Content-Type: application/json
X-Webhook-Timestamp: 1784464245
X-Webhook-Signature: v1=0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef
```

```
{
  "message_id": "01JEXAMPLE0000000000000000",
  "status": "delivered",
  "client_reference": "order-1042",
  "delivered_at": "2026-07-19T12:30:44.987654Z",
  "timestamp": "2026-07-19T12:30:45.123456Z"
```

```
}
```

Success response

Any 2xx response acknowledges the event. The receiver's response body and headers are not defined by this contract.

Response headers

None are defined by this contract.

Response body

None is required by this contract.

Possible errors

Receiver-defined. MHI Gateway does not define the receiver's error schema.

HTTP status codes

Any 2xx acknowledges delivery.

Notes

The signature input is the exact byte sequence `<timestamp>.<raw-request-body>`. Receivers must compare signatures in constant time and reject timestamps more than five minutes outside current time.

The outbound timeout is 10 seconds. RC1 makes exactly one delivery attempt and does not schedule retries. Events are emitted only for delivered, failed, expired, and rejected.

Best practices

Verify the signature against the raw body before parsing JSON, enforce replay protection, and return 2xx promptly after durable handoff.

Related endpoints

- [Replace delivery webhook configuration](#)
- [Retrieve normalized message status](#)

10 Common Schemas

All reusable OpenAPI schemas are documented below. Unless a property explicitly permits null, Nullable is No. The current schemas do not declare nullable properties.

10.1 CorrelationId

String used for request correlation.

Name	Type	Required	Nullable	Constraints	Description
value	string	Context-dependent	No	1-100 characters; ^[A-Za-z0-9][A-Za-z0-9._: -]{0,99}\$	Correlation identifier

10.2 MessageId

Public message identifier.

Name	Type	Required	Nullable	Constraints	Description
value	string	Context-dependent	No	Exactly 26 characters; ^[0-9A-HJKMNP-TV-Z]{26}\$	Public message ULID

10.3 MessageStatus

Closed public message-status vocabulary.

Name	Type	Required	Nullable	Constraints	Description
value	string	Context-dependent	No	Enum: queued, submitted, delivered, failed, expired, rejected, unknown	Normalized public status

10.4 Timestamp

Name	Type	Required	Nullable	Constraints	Description
value	string	Context-dependent	No	Format: date-time	UTC RFC 3339 timestamp; persisted resources retain microseconds

10.5 MessageSubmission

Object with `additionalProperties`: false.

Name	Type	Required	Nullable	Constraints	Description
recipient	string	Yes	No	^[1-9][0-9]{7,14}\$	E.164 recipient
message	string	Yes	No	1-4096 characters	SMS message text
sender_id	string	No	No	1-191 characters; ^[\x00-\x1F\x7F]+\$	Sender identifier
client_reference	string	No	No	1-100 characters; restricted correlation pattern	Client metadata

10.6 MessageAccepted

Object with `additionalProperties`: false.

Name	Type	Required	Nullable	Constraints	Description
message_id	MessageId	Yes	No	Message ID pattern	Public message identifier
status	MessageStatus	Yes	No	Public status enum	Initial normalized status
client_reference	string	No	No	No additional OpenAPI constraint	Client metadata

Name	Type	Required	Nullable	Constraints	Description
created_at	Timestamp	Yes	No	UTC RFC 3339	Creation time
correlation_id	Correlation Id	Yes	No	Correlation ID constraints	Original submission correlation ID; retained on replay

10.7 MessageDetails

Object with additionalProperties: false.

Name	Type	Required	Nullable	Constraints	Description
message_id	MessageId	Yes	No	Message ID pattern	Public message identifier
recipient	string	Yes	No	No additional OpenAPI constraint	Message recipient
sender_id	string	No	No	No additional OpenAPI constraint	Sender identifier
client_reference	string	No	No	No additional OpenAPI constraint	Client metadata
status	MessageStatus	Yes	No	Public status enum	Current normalized status
created_at	Timestamp	Yes	No	UTC RFC 3339	Creation time
submitted_at	Timestamp	No	No	UTC RFC 3339	Provider submission time
finalized_at	Timestamp	No	No	UTC RFC 3339	Terminal transition time
correlation_id	CorrelationId	Yes	No	Correlation ID constraints	Current request correlation ID

10.8 MessageStatusResource

Object with additionalProperties: false.

Name	Type	Required	Nullable	Constraints	Description
message_id	MessageId	Yes	No	Message ID pattern	Public message identifier
status	MessageStatus	Yes	No	Public status enum	Current normalized status
occurred_at	Timestamp	Yes	No	UTC RFC 3339	Authoritative status occurrence time
client_reference	string	No	No	No additional OpenAPI constraint	Client metadata
correlation_id	Correlation Id	Yes	No	Correlation ID constraints	Current request correlation ID

10.9 BatchId

Name	Type	Required	Nullable	Constraints	Description
value	string	Context-dependent	No	UUIDv4; lowercase pattern <code>^[0-9a-f]{8}-[0-9a-f]{4}-4[0-9a-f]{3}-[89ab][0-9a-f]{3}-[0-9a-f]{12}\$</code>	Replay-stable tracking metadata; not a public resource

10.10 BulkSubmission

Object with additionalProperties: false.

Name	Type	Required	Nullable	Constraints	Description
client_reference	string	No	No	1-100 characters; restricted correlation pattern	Batch-level client metadata
messages	array of BulkMessageCandidate	Yes	No	1-100 items	Ordered candidates; order is significant

10.11 BulkMessageCandidate

Object with `additionalProperties`: `false`. Candidate fields are independently validated after top-level acceptance.

Name	Type	Required	Nullable	Constraints	Description
recipient	string	No	No	Evaluated as an item candidate	Recipient candidate
message	string	No	No	Evaluated as an item candidate	Message candidate
sender_id	string	No	No	Evaluated as an item candidate	Sender candidate
client_reference	string	No	No	Evaluated as an item candidate	Per-item client metadata

Missing, malformed, or excessive values produce an item error rather than rejecting valid siblings.

10.12 BulkAcceptedResult

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
index	integer	Yes	No	0-99	Original zero-based input index
message_id	MessageId	Yes	No	Message ID pattern	Accepted message identifier
status	string	Yes	No	Constant: <code>queued</code>	Initial accepted status
client_reference	string	No	No	1-100 characters	Per-item client metadata

10.13 BulkRejectedResult

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
index	integer	Yes	No	0-99	Original zero-based input index
error	BulkItemError	Yes	No	Bulk item error schema	Safe item rejection

10.14 BulkItemError

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
code	string	Yes	No	Enum: <code>INVALID_REQUEST</code> , <code>INVALID_RECIPIENT</code> , <code>INVALID_SENDER_ID</code> , <code>MESSAGE_TOO_LONG</code> , <code>SERVICE_UNAVAILABLE</code> , <code>INTERNAL_ERROR</code>	Stable item error code
message	string	Yes	No	No additional OpenAPI constraint	Safe item error message
details	object	Yes	No	Additional properties allowed	Safe structured details

10.15 BulkItemResult

Name	Type	Required	Nullable	Constraints	Description
value	BulkAcceptedResult or BulkRejectedResult	Yes in BulkResult.results	No	oneOf exactly one result representation	Result for one input candidate

10.16 BulkResult

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
batch_id	BatchId	Yes	No	UUIDv4	Replay-stable tracking identifier
client_reference	string	No	No	1-100 characters	Batch-level client metadata
accepted	integer	Yes	No	0-100	Accepted item count
rejected	integer	Yes	No	0-100	Rejected item count
results	array of BulkItemResult	Yes	No	1-100 items	Input order; one result per candidate

`accepted` + `rejected` equals the length of `results`.

10.17 DeliveryWebhookWrite

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
url	string	Yes	No	Format: uri; HTTPS mandatory in production	Delivery receiver URL
secret	string	Yes	No	Minimum 32 bytes; write-only	HMAC secret; old secret remains valid for 24 hours after replacement
enabled	boolean	Yes	No	Boolean	Whether delivery is enabled

10.18 DeliveryWebhookRead

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
url	string	Yes	No	Format: uri	Delivery receiver URL
enabled	boolean	Yes	No	Boolean	Whether delivery is enabled
created_at	Timestamp	Yes	No	UTC RFC 3339	Configuration creation time
updated_at	Timestamp	Yes	No	UTC RFC 3339	Configuration update time

10.19 DeliveryWebhookEvent

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
message_id	MessageId	Yes	No	Message ID pattern	Public message identifier
status	string	Yes	No	Enum: delivered, failed, expired, rejected	Terminal public status
client_reference	string	No	No	No additional OpenAPI constraint	Client metadata
delivered_at	Timestamp	No	No	UTC RFC 3339	Delivery time when present
timestamp	Timestamp	Yes	No	UTC RFC 3339	Event timestamp

10.20 ErrorBody

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
code	string	Yes	No	Official request-level error enum	Stable error code
message	string	Yes	No	No additional OpenAPI constraint	Sanitized human-readable message
details	object	Yes	No	Additional properties allowed	Safe structured details
correlation_id	CorrelationId	Yes	No	Correlation ID constraints	Current request correlation ID

10.21 ErrorResponse

Object with `additionalProperties`: `false`.

Name	Type	Required	Nullable	Constraints	Description
error	ErrorBody	Yes	No	Error body schema	Request-level error

11 Response Headers

11.1 API responses

Header	Successful responses	Error responses	Description
X-Request-ID	Present	Present	Unique identifier for the current HTTP request
X-Correlation-ID	Present	Present	Current request correlation identifier
Content-Type	application/json	application/json	Response media type

OpenAPI explicitly models X-Correlation-ID on successful operations. The frozen common protocol requires both identifiers on every HTTP response.

11.2 Idempotent replay

On a single-message replay:

- X-Request-ID identifies the current replay HTTP request;
- X-Correlation-ID identifies the current replay request correlation;
- body correlation_id remains the original submission correlation.

On a bulk replay, batch_id and the original body remain stable while the response identifier headers describe the current HTTP request.

11.3 Webhook acknowledgment

The receiving application chooses its response headers. MHI Gateway does not define webhook acknowledgment headers.

12 Error Codes

12.1 Request-level errors

Only the following codes are present in the OpenAPI `ErrorBody` enum.

HTTP status	Code	Meaning
401	AUTHENTICATION_FAILED	Credential is absent or invalid
403	FORBIDDEN	Authenticated principal is not permitted
400	INVALID_REQUEST	Request is invalid
422	INVALID_RECIPIENT	Recipient is invalid
422	INVALID_SENDER_ID	Sender identifier is invalid
422	MESSAGE_TOO_LONG	Message exceeds the maximum length
409	IDEMPOTENCY_CONFLICT	Key is bound to different canonical input
404	MESSAGE_NOT_FOUND	Message is absent from the authenticated scope
422	WEBHOOK_CONFIGURATION_INVALID	Webhook configuration is invalid
429	RATE_LIMIT_EXCEEDED	Rate limit exceeded
503	SERVICE_UNAVAILABLE	Service is temporarily unavailable
500	INTERNAL_ERROR	Sanitized internal failure

Endpoint-specific HTTP response status sets are defined in [Endpoint Reference](#). Do not assume that every official code is returned by every operation.

12.2 Bulk item errors

Bulk item rejections contain only:

Code	Meaning
INVALID_REQUEST	Candidate request is invalid
INVALID_RECIPIENT	Candidate recipient is invalid
INVALID_SENDER_ID	Candidate sender is invalid
MESSAGE_TOO_LONG	Candidate message exceeds the maximum length
SERVICE_UNAVAILABLE	Candidate could not be processed because service is unavailable
INTERNAL_ERROR	Candidate evaluation encountered an internal failure

Bulk item errors contain `code`, `message`, and `details`; they do not contain the request-level `correlation_id`.

13 Status Values

13.1 Public message statuses

Status	Terminal	Meaning
queued	No	Accepted or processing without durable provider-submission evidence
submitted	No	Durable provider submission or acceptance evidence exists
delivered	Yes	Delivered
failed	Yes	Failed
expired	Yes	Expired
rejected	Yes	Rejected
unknown	No	Authoritative outcome is unavailable or contradictory

13.2 Allowed transitions

Current status	Allowed next statuses
queued	submitted, delivered, failed, expired, rejected, unknown
submitted	delivered, failed, expired, rejected, unknown
unknown	delivered, failed, expired, rejected
delivered	delivered for identical evidence
failed	failed for identical evidence
expired	expired for identical evidence
rejected	rejected for identical evidence

Terminal states are immutable. A contradictory late terminal event does not rewrite public history.

13.3 Webhook statuses

Delivery webhook events use only:

```
delivered
failed
expired
rejected
```

No webhook event is emitted for queued, submitted, or unknown.

14 Appendices

Appendix A: Endpoint matrix

Method	Path	Request schema	Success schema	Success status
POST	/messages	MessageSubmission	MessageAccepted	202
POST	/messages/bulk	BulkSubmission	BulkResult	202
GET	/messages/{message_id}	None	MessageDetails	200
GET	/messages/{message_id}/status	None	MessageStatusResource	200
PUT	/webhook	DeliveryWebhookWrite	DeliveryWebhookRead	200
GET	/webhook	None	DeliveryWebhookRead	200
POST	Configured receiver URL	DeliveryWebhookEvent	Receiver-defined	Any 2xx

Appendix B: Reusable parameters

OpenAPI name	Wire name	Location	Required	Schema
IdempotencyKey	Idempotency-Key	Header	Yes on submission	String, 1-191 visible ASCII characters
CorrelationId	X-Correlation-ID	Header	No	CorrelationId
MessageId	message_id	Path	Yes	MessageId
WebhookTimestamp	X-Webhook-Timestamp	Header	Yes on webhook	Integer int64, Unix seconds
WebhookSignature	X-Webhook-Signature	Header	Yes on webhook	^v1=[0-9a-f]{64}\$

Appendix C: Reusable OpenAPI responses

Component	Description
ValidationError	Request validation failed
AuthenticationFailed	Credential is absent or invalid
Forbidden	Authenticated principal is not permitted
NotFound	Resource is absent from the authenticated scope
IdempotencyConflict	Key is already bound to different canonical input
RateLimited	Rate limit exceeded
InternalServerError	Sanitized internal failure
ServiceUnavailable	Service is temporarily unavailable

Every component uses ErrorResponse.

Appendix D: Identifier formats

Identifier	Format
API credential	mhi_<environment>_<12-character-prefix>.<48-character-secret>
Correlation ID	1-100 characters; restricted ASCII pattern
Message ID	26-character public ULID pattern
Batch ID	Lowercase UUIDv4
Idempotency key	1-191 visible ASCII characters
Webhook signature	v1= plus 64 lowercase hexadecimal characters

Appendix E: Source precedence and route inventory

This reference follows OpenAPI as the authoritative source. The application route inventory contains an additional collection route, GET /messages, that is not present in OpenAPI and is therefore not part of this public API reference.

Appendix F: Related resources

- [OpenAPI 3.1](#)
- [API v1 Contract](#)
- [Developer Integration Guide](#)
- [Client examples](#)

End of MHI Gateway API Reference v1.0