webMethods API Cloud 10.5 Readme

November 2019

This file contains important information you must read before using webMethods API Cloud API Gateway 10.5. You can find user documentation for API Cloud on the Documentation website or the TECHcommunity website. At those locations, you can also find suite-related security and globalization information.

Included in this file is information about functionality that has been added, removed, deprecated, or changed for this product. Deprecated functionality continues to work and is supported by Software AG, but may be removed in a future release. Software AG recommends against using deprecated functionality in new projects.

1.0 Critical Information

This section lists any critical issues for the current release that were known when this readme was published. For critical information found later, go to the Knowledge Center on the Empower website.

2.0 Known Issues

This section lists any issues for the current release that were known when this readme was published. For known issues found later, go to the Knowledge Center on the Empower website.

3.0 Usage Notes

This section provides any additional information you need to work with the current release of this product.

This release is based on the 10.5 on-premise release.

The following functionalities have certain restrictions in webMethods API Cloud API Gateway instance:

- API support
  webSocket API is not supported.
- Policy support
  The following policies are not supported in a cloud instance as they are relevant only for an on premise deployment:
  - Enable JMS/AMQP
  - JMS/AMQP Routing
  - JMS/AMQP Properties
  - Authorize User
- Policy Properties support
  The following policy properties are not supported in API Cloud API Gateway instance:
  - Audit Log, JDBC, Digital Events, and SNMP destinations are not available in the following policies:
    - Log Invocation
    - Monitor Service Performance
    - Monitor Service Level Agreement
    - Throttling Traffic Optimization

- In the Identify & Authorize Application policy, the HTTP Basic Authentication is not supported if Identity Provider(IdP) is configured in webMethods Integration Cloud (wMIC).
- The following properties are not available in the Inbound Authentication - Message policy
  - Validate SAML Audience URL
  - Require SAML Token under Token Assertions
- The Run as user property is not available in the following policies
  - Invoke webMethods IS Service
  - IS Service alias
  - Request Transformation
  - Response Transformation
  - Conditional Error Processing

- Administration support
  - Access URLs
    Tenants can access the API Cloud API Gateway instance (both the UI and runtime invocation) **only** using the URL provided by Software AG. This implies the following restrictions for the tenant:
    - Ports section is not available since they cannot be manipulated.
    - Load Balancer URLs section is not available since they cannot be manipulated.
  - Cache configuration support is not available.
  - Licensing support is not available
  - Clustering configuration support is not available.
  - Application logs section that contains configuring aggregation of logs is not supported.
  - OAuth
    - If Identity Provider(IdP) is configured in WmIC, implicit grant and authorization code grant modes of OAuth are not supported.
  - Destinations
    The following destinations have restrictions in API Cloud API Gateway instance:
    - Audit Log, Database, Digital Event Services (DES) and third party SNMP server are not available since they are relevant only for on premise cases.

        - API Portal settings are auto populated and disabled when API Portal is provisioned as part of the API Cloud.
        - For an Email destination, only templates can be configured since API Gateway Cloud instance has a predefined email server that cannot be changed.
    - Settings
        - Outbound Proxy section is not available under General configuration as it is relevant only for an on premise deployment.
        - Kibana port cannot be updated as it is predefined and SAML SSO section is not available under the system settings section.
    - Few Extended settings are not available.
    - System Information in the About page is not included.
- The Send Digital Events notification setting under Quota management is unavailable.
- Analytics support
    - Runtime event data cannot be archived or restored in API Cloud API Gateway instance.
    - Cache statistics is not available.
    - Application logs are not available.
- Connectivity
    - Service development is not possible in API Gateway cloud, that is, Designer cannot be connected in API Cloud API Gateway instance.
    - Integration Server console cannot be accessed. This means that all the configurations including logging is not available
    - Reverse Invoke from an on premise instance is not supported.
    - Paired gateway setup is not supported in a cloud instance. Advanced Edition is the default hosted solution.
    - 2-way SSL authentication is not supported

4.0 Fixes Included in Each Release

This section lists the latest fix level that has been included in each release for each product component. A release is listed in this section only if changes occurred in that release. Go to the Knowledge Center on the Empower website for detailed information about fixes.

5.0 Other Resolved Issues

This section lists the issues that were resolved in each release but were not part of the fixes listed in the previous section. A release is listed in this section only if changes occurred in that release.

6.0 Documentation Changes

This section describes significant changes to the documentation, such as the addition, relocation, or removal of product guides, online help, chapters, or other major content. A release is listed in this section only if changes occurred in that release.

Release 10.3

The following artifact has been introduced for API Cloud API Gateway instance 10.3:

- API Cloud: API Gateway Help: This is the HTML version of the User's Guide and online help available on Empower.

Release 10.1

The following artifacts have been introduced for API Cloud API Gateway instance 10.1:

- API Cloud: API Gateway Quick Start Guide: This is single page PDF output that gives an overview of setting up API Cloud API Gateway instance.
- API Cloud: API Gateway User's Guide: This is the PDF version of the online help included in the product.
- API Cloud: API Gateway Online Help: This is the HTML version of the help included in the product.

7.0 Terminology Changes

A release is listed in this section only if changes occurred in that release.

8.0 Added, Removed, Deprecated, or Changed Items

This section lists features, functionality, controls, portlets, properties, or other items that have been added, removed, deprecated, or changed. A release is listed in this section only if changes occurred in that release.

Release 10.5

Added Item	Description
Custom Runtime Policies	API Providers can now invoke any external services, which can act as a runtime policy as part of the policy enforcement and thus can support custom runtime policies. Custom policies can be included in the stages such as, Identify and Access or Payload processing stages, or Routing stage. AWS Lambda functions also can be considered for custom policies.
Team work Support	Team work support is to provide access control based on team-specific privileges in the deployments where multiple teams work on a single API Gateway instance. Assets of type API, Application, Package, Plan would be team-specific in such deployments and deployments where teams is not applicable, this can be switched off. Team work support is available for Software AG Cloud provisioned tenants only.
API First	API-first is an approach where the design and development of an API comes before the implementation. API Gateway can now cater provider-complaint specification that can be used to register API first in API Gateway as part of API-first approach.
Change ownership of Assets	Ownership of API and Application type assets can be transferred to a different user and can be implemented with Approval flow if desired. This would help to overcome the unavailability of specific data in the case where the current owner is not available in the system.
Governed API development	APIs provided by CentraSite are considered read-only if a CentraSite destination is configured. If there is no CentraSite destination there is no connection to CentraSite and therefore no read-only restriction needs to be enforced. Scopes and policies can still be updated in API Gateway.

Release 10.4

Added Item	Description
Import and Export Enhancements	Import and export support that was limited to some assets is now enhanced to include all assets and configurations so that users can easily move the configurations across instances.
Staging and Promotion Enhancements	Staging and promotion support that was limited to some assets is now enhanced to include all assets and configurations so that users can easily move the configurations across instances. Aliases can be configured with stage details.
Support Certificates in Custom Headers	Application identification is enhanced to get certificates sent through Custom HTTP header in order to identify the application. Custom header can be configured as part of extended settings of Administration
Support API Composition in API Mashups	API providers can configure to invoke multiple APIs as part of mashup step and aggregate the response that is passed to the next step. Similarly responses of different steps can be aggregated and sent as single output to the client.
Microgateway Management in API Gateway	API Gateway displays list of live Microgateways registered to it and are now able to retrieve details about list of assets, and configurations of each Microgateway.

Changed Item	Description
Application Identification	In case of Application identification failure, error message is changed from Unable to identify the application for the request to Unauthorized application request.

Release 10.3

Added Item	Description
Open API Support	Users can create an API by importing an open API document file or URL in API Gateway. OpenAPI Specification (formerly Swagger Specification) is an API description format for REST APIs.
Support for API Mashups	Individual microservices and APIs can be composed into one mashed up API. API Gateway handles a request by invoking multiple microservices and aggregating the results and providing a final response.

Added Item	Description
Support Async APIs	APIs, which take longer than usual invocation time, may end up with Read Time out. API Gateway could enforce policies to use the callback URL defined for the APIs.
Support AMQP protocol	Support AMQP as an inbound and outbound endpoint for API Gateway APIs of type SOAP and REST. AMQP is open standard for passing messages between applications and provides standard messaging protocol across platforms.
API hot deploy	API updates can be done without deactivating or affecting the ongoing requests. Each request finishes without being affected by updates to the API and policy definition.
Support runtime service registries	API Gateway APIs can be published to service registries and clients can get the endpoints from service registry. APIs routing endpoint can be configured with service registry to discover endpoint from registry during outbound.
Security enhancements	Security configuration is unified for OAuth, OpenID and JWT configuration, and is simplified. Support for multiple active Authorization servers simultaneously is included. Added capability to register clients dynamically in third-party Authorization servers. Support for third-party clients introspection. PKCE client application support for third-party Authorization servers. Mapping of OAuth scopes with API scopes.

Release 10.2

Added Item	Description
API Tagging	APIs or its resources and operations can be tagged. You can use the tags for searching artifacts in API Gateway and publish the tags along with the API to API Portal. API creation using Swagger can acquire the tags from the swagger file and also API export should include the assigned tags.
Bulk Publish, Unpublish and Delete	You can publish, unpublish or delete more than one API at a time to API Portal.
File attachments support for API	APIs can be attached with supporting files as attachments and the attached files are available in API Portal after publishing to the Portal.

Added Item	Description
JWKS endpoint for JSON Web Tokens	As an ID provider, API Gateway provides the JWKS endpoint that helps the relying parties to fetch the certificates that can be used for validation of the JSON Web tokens.
Application suspension	You can now suspend applications to deactivate the runtime access to the applications in API Gateway and the same application can be activated again.
CORS Support in API gateway	API Gateway can process cross origin requests sent by clients as inbound policy and also as transparent mode of native service processing cross origin requests.
Specification for Invoke IS Service	You can now define IS Service to get and set headers, status code, body, and other MessageContext variables using the specification in the service and do not have to write code to extract the variables.
Enhance Transaction events	Transaction events are enhanced to log headers and query parameters of request and response along with the payload.
Data masking	API Gateway's data masking policy can be configured to mask or filter specific data in request and response messages and also mask the data in transaction events.
JSON Schema and JSON Path Support	JSON payload can be evaluated for schema validation and JSON path can be used in policies like content-based routing, error processing, and identify application.
Audit logging support	Audit logging would capture user activities in API Gateway for API, application, approvals, and user management. Audit logs would capture who has done the action and when. These logs help in securing the system.

Added Item	Description
API Monetization	Plans and packages can be managed by quotas, usage, and rate limits with soft and hard limits. Consumers can subscribe to plans and monitor usage and re-subscribe as required.
Transaction metering across stages	API Gateway now supports metering of transactions across stages. You can specify alert configurations to notify when the number of transactions across the stages reaches a specified limit. The notification can be delivered through email and/or web hooks.

9.0 Copyright Information

10.0 Support

Visit the Empower website to learn about support policies and critical alerts, read technical articles and papers, download products and fixes, submit feature/enhancement requests, and more.

Visit the TECHcommunity website to access additional articles, demos, and tutorials, technical information, samples, useful resources, online discussion forums, and more.

YAIC-RM-105-20191114