

webMethods API Gateway 10.2 Readme

April 2018

This is an innovation release. Innovation releases have a much shorter support cycle than standard releases. To learn more, please visit <http://empower.softwareag.com/innovationrelease/>

This file contains important information you must read before using webMethods API Gateway 10.2. You can find system requirements, user documentation, and installation and upgrade instructions 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.....	2
2.0	Known Issues.....	2
3.0	Usage Notes.....	3
4.0	Fixes Included in Each Release.....	4
5.0	Other Resolved Issues.....	4
6.0	Documentation Changes	4
7.0	Terminology Changes	5
8.0	Added, Removed, Deprecated, or Changed Items.....	5
9.0	Copyright Information.....	11
10.0	Support.....	11

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](#).

- YAI-7367
CentraSite deployed API key is encoded.
When an application is deployed along with the API from CentraSite to API Gateway, the API key in the API Gateway application is shown as encoded.
- YAI-7363
OAuth2 CentraSite deployment scope is not set.
Scope is not set for an application in API Gateway when deployed along with the API, the application is consuming, from CentraSite.
- YAI-7288
Suspended application is logged as "Unknown" application in API Gateway analytics dashboard.
For suspended application, API invocation fails with an error message but the same is logged as "Unknown" application in API Gateway analytics dashboard.
- YAI-7320
Data is not masked for invocation failure message.
When an API is configured for data masking, in case of failure, the API response does not mask the configured data.
- YAI-7350
Update alias by import does not update the alias value in existing API.
While importing an alias, even though the **Alias overwrite existing** option is selected in advanced options, the alias value for the existing APIs are not updated.
- YAI-7189
API associated with a package is allowed to be deleted.
An API, which is associated with a package, is deleted and imported again using export archive of the API, the association of API and Package is created automatically.

3.0 Usage Notes

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

- YAI-1286
Activating an API, with big WSDL, from Gateway UI displays StackOverFlowError.
When you see a StackOverFlowError while activating an API, increase the thread stack size in `IS_Installed_Folder\profiles\IS_default\configurations\wrapper.conf` in IS using the command:
`wrapper.java.additional.7=-Xss2048k`
- Before using API Gateway, consider the following points:
 - While using API Gateway on HP-UX OS , consider increasing Java heap size in `<SAG_install_dir>/profiles/IS_default/configuration/custom_wrapper.conf`:
`wrapper.java.initmemory=512`
`wrapper.java.maxmemory=2048`
Use different Java executable in `<SAG_install_dir>/profiles/IS_default/configuration/wrapper.conf`:
`wrapper.java.command=<SAG_install_dir>/jvm/jvm/jre/bin/IA64W/java_q4p`
 - API Gateway package in Integration Server, cannot co-exist with the WmMediator or WmCloudStreams packages. WmMediator and WmCloudStreams packages must be disabled for API Gateway to function properly.
 - webMethods API Gateway combines current webMethods Enterprise Gateway and webMethods Mediator capabilities in a single product. API Gateway offers the same capabilities within a simplified architecture. It also removes the dependency on CentraSite for API definition and policy definition.
 - API Gateway comes in two editions. The Standard edition allows users to define threat protection policies, and provides analytics for threat protection use cases. Typically Standard editions are deployed in DMZ.
Full edition supports all use cases of Standard edition, supports managing APIs, consumer applications, API-level policies, and managing API packages and plans.
 - When API Gateway and Event Data Store are already running and IP address is changed, connection between API Gateway and Event Data Store is lost. Restart the Event Data Store to reconnect to API Gateway.

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.

Release 10.1

- YAI_10.1_Fix6

Release 10.0

- YAI_10.0_Fix9

Release 9.12

- YAI_9.12_Fix7

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 10.0

The following artifacts have been introduced for API Gateway 10.0:

- webMethods API Gateway Quick Start Guide: This is single page PDF output that gives an overview of setting up API Gateway.

Release 9.12

The following artifacts have been introduced for API Gateway 9.12:

- webMethods API Gateway Online Help
- webMethods API Gateway User's Guide: This guide describes how you can use API Gateway and other API Gateway components to effectively manage APIs for services that you want to expose to

consumers, whether inside your organization or outside to partners and third parties.

- **webMethods API Gateway Configuration Guide:** This guide describes how you can configure API Gateway and other API Gateway components to effectively manage APIs for services that you want to expose to consumers, whether inside your organization or outside to partners and third parties.

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 10.2

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.
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.
HTTP Client for Elastic Search	Relaxes the hard limitation of using the Elastic search shipped along with API Gateway product; you can use other elastic search instance configured with API Gateway

Added Item	Description
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.
Caching enhancements	You can manage different caches of API Gateway to auto scale or allocate static percentage of data to be held in cache.
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.
User profile management	You can now configure your preferences like name, email passwords, and display language.
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.
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.

Release 10.1

Added Item	Description
Migration from Mediator to API Gateway	<p>APIs and associated data can be published from CentraSite to API Gateway 10.1 version.</p> <p>This allows users to publish Virtual Services of SOAP and REST with applied policies, consumer applications, runtime alias to API Gateway, which play the role of policy enforcement point and replace Mediator.</p>
Migration from Enterprise Gateway to API Gateway	<p>Enterprise Gateway configurations and Rules can be migrated to API Gateway, which replace and play the role of Enterprise Gateway.</p>
Staging and Promotion support	<p>You can now promote assets from one stage to another. API Gateway uses webMethods Deployer for promoting assets across stages. Promoting an asset involves calculating its dependencies and promoting them unless explicitly specified by the user. Stage-specific configurations and alias values can be modified to respective values.</p> <p>API Gateway assets can be managed with version control system and perform scheduled or automatic promotion to stages as configured.</p>
Support for SOAP over JMS	<p>Support JMS protocol of Inbound and Outbound for SOAP. Allow JMS-HHTTP bridging between Inbound and Outbound.</p>
Backup and Restore	<p>Backup API Gateway assets and configuration using command line and you can restore the backed up data.</p>
Transaction based licensing	<p>License model based on transactions and appropriate alerts can be implemented</p>
Approval model for applications	<p>Approval model can be implemented for creating or updating applications, associating applications with APIs, and subscribing to packages.</p>
API Mocking	<p>Mocking mode allows users to make mock calls to APIs. User can specify API response for each resource or operation and can set status codes for responses. API responses can be configured on conditional basis too.</p>

Added Item	Description
Support 3rd party OAuth providers	Users can use 3rd party Authorization Servers for authenticating API invocations using OAuth2 Third party OAuth2 providers like OKTA and Ping Federate can be used for OAuth2 authentication.
Support JSON Web Tokens	API Gateway can authenticate clients using JSON Web Tokens supplied during invocations.
Open ID Support	API Gateway can authenticate clients using Open ID Tokens supplied during invocations.
HTTP Header Validation	Providers can mandate consumers to send HTTP headers and values defined in policy for API Invocations.

Release 10.0

Added Item	Description
API Versioning	New version for an API can be created. Different versions of an API can be viewed and invoked.
SOAP to REST transformation	API Provider can enable some of the operations of SOAP service as REST endpoints. These operations can be invoked with different paths and the operation path can contain Path parameters that can be saved as templates and can be hierarchical. The operation can be invoked in a method other than POST.
API export and import	APIs in API Gateway can be exported and imported into a different API Gateway. This implies that the export archive for an API includes all the information to establish an API in the importing API Gateway.
Support Service Result Cache	Service result of the first invocation is cached when the criteria defined in the policy is met. Subsequent requests are from cache and do not require to go to native service for every similar invocation.

Added Item	Description
Schema Validation Support	Validates the incoming requests and responses against a schema referenced in the WSDL for SOAP APIs. For REST API, user should be able to validate incoming requests and responses against the specified schema.
API usage reports and dashboards	Package-level and API-specific usage and utilization reports. API Gateway provides number widgets for package invocations and API invocations.
Archive purge and restore events data	Administrators can archive and purge events data to a configured file location. The archived data is restored from the created archives.
Resources or Operation level policies	Policies can be applied to one or more resources or operations and must be applied on an API always. Scope can be created with a collection of resources, methods or operations of an API and policies can be applied to the scope to apply to the specific operation or resources.
Global policies and policy templates	Global Policy is a common policy that can be associated to multiple APIs based upon the criteria defined for the policy. Policy Template is a base template defined, which can be imported in multiple APIs.
SAML Authentication	APIs can be applied with SAML authentication policies at Inbound and Outbound. Bearer and Holder of Key SAML subject confirmation are supported for SAML 1.0 and 2.0 versions.
Kerberos Authentication	Kerberos authentication is supported at message and transport level for SOAP APIs and at transport level for REST APIs. APIs can be applied with Kerberos authentication policies at Inbound and Outbound.
XML Threat Protection Support	API Gateway application should be resilient to attacks through XML payload. XML payloads sent through external port go through the XML threat protection filter when the rule is defined and enabled.

Added Item	Description
JSON Threat Protection Support	API Gateway application should be resilient to attacks through JSON payload. JSON payloads sent through external port go through the JSON threat protection filter when the rule is defined and enabled.

Release 9.12

Added Item	Description
API CRUD	Both REST and SOAP APIs can be imported. Swagger and RAML are supported formats for REST and WSDL for SOAP. REST APIs can be created from scratch as well.
Policies and Aliases CRUD	Both threat protection and API-specific policies based in selected edition. For more information, see documentation for supported policies. Create and manage aliases that improve the reuse and maintenance.
Consumer Applications CRUD	Manage consumer applications and associations with APIs.
Packages and Plans	Organizations can group APIs and define enforcements on the same as a single unit, which can be subscribed by developers.
API Portal Integration	APIs can be published to API Portal from API Gateway for the developers reach.
Analytics	API Gateway provides dashboards for greater insights on various topics like Summary, Trends, Consumer applications, and Threat protection.

9.0 Copyright Information

Copyright © 2018 Software AG, Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

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.

YAI-RM-102-20180417