

webMethods API Gateway 10.0 Readme

April 2017

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 10.0. 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.....	5
6.0	Documentation Changes	5
7.0	Terminology Changes	5
8.0	Added, Removed, Deprecated, or Changed Items.....	6
9.0	Copyright Information.....	8
10.0	Support.....	9

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-3176
SOAP To REST: Namespace inline edit displays an error.
Inline edit of XPath namespace declaration in SOAP to REST displays an error.
There is no workaround for this issue.
- YAI-3185
API version cannot be created for an API with scopes.
An error occurs and the new version of an API is not created when an API with scopes is versioned.
There is no workaround for this issue.
- YAI-3088
Service result cache displays Class Not found error in clustered environment.
When a service is configured with the Service Result Cache policy and the cache is invoked to receive the response stored in the cache, an error displays if API Gateway is in a clustered environment.
There is no workaround for this issue.
- YAI-3079
Fault handling is not engaged on SOAP API's.
Conditional Error Processing policy configured for API is not engaged during runtime for SOAP-based services. A default error message is returned when a fault occurs.
There is no workaround for this issue.
- YAI-2995
Duplicate endpoints and communities are displayed while publishing APIs.
While publishing the API from API Gallery page, the publish dialog appears with endpoint and community information. This information is duplicated if you click the Publish button more than once.
There is no workaround for this issue.
- YAI-3118
While importing existing applications, existing API in the list are not updated.
While importing an application that already exists with registered APIs, the registered APIs are not updated.
There is no workaround for this issue.

- YAI-2952
Not able to import versioned APIs with same name.
Import of an API with two versions fails for the first version, whereas the latest version of the API is imported successfully.
There is no workaround for this issue.
- YAI-2985
Deleting an API with a scope policy, does not delete the scope policy.
While deleting an API with a scope policy, the scope policies are not deleted even after API is deleted.
There is no workaround for this issue.
- YAI-3100
Invoking an API in API Gateway that has the Outbound Authentication - Message policy enforced displays an error at runtime.
When Outbound Authentication - Message policy is configured without security configuration for an API, invoking the API displays an error at run-time.
There is no workaround for this issue.
- YAI-3117
Refresh of API access key or OAuth2 credentials on a clustered environment does not update the information on cluster nodes.
When API Key or OAuth tokens are refreshed in a clustered environment, keys are updated only on the node where refresh token is triggered. The refreshed tokens are not updated on all nodes.
There is no workaround for this issue.
- YAI-3060
OAuth tokens are not applicable at scope level.
Providers cannot restrict API access at scope level with OAuth. OAuth tokens can be applied only at the API level and not at API scope level.
There is no workaround for this issue.

3.0 Usage Notes

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

- YAI-1286
Activate of 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`
- YAI-1430
SOAP API with same name as a WSD cannot be activated.
An error occurs while activating a SOAP API when the API name is same as a WSD in Integration

Server.

- Before using API Gateway, consider the following points:
 - 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 EventDatastore are already running and IP address is changed, connection between API Gateway and EventDatastore is lost. Restart the EventDatastore 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 9.12

- YAI_9.12_Fix4

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 10.0

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.
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.

Added Item	Description
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.
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.

Added Item	Description
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 © 2017 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-100-20171013