webMethods API Gateway 10.1 Readme

October 2017

This file contains important information you must read before using webMethods API Gateway 10.1. 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

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-5057

  Unable to import an API with mandatory password fields in policies.

  Importing an exported archive of an API that has policies with mandatory password fields fails.

  There is no workaround for this issue.

- YAI-5064

  Application created by one user cannot be viewed by other user.

  Users can see applications created by other users, in the applications list or in search results, but cannot see the application details view.

  There is no workaround for this issue.

- YAI-4974

  Exceptions are logged during startup after migrating Event Data Store.

  After migrating 10.0 Event Data Store to 10.1, exceptions are logged during server startup and Event Data Store startup.

  There is no workaround for this issue.

- YAI-5191

  Issue in loading the keystore and truststore configurations.

  In a clustered environment of an API Gateway setup, with keystore and truststore configuration done on a node, the keys of the keystore in the configuration of the other nodes do not get loaded.

  There is no workaround for this issue.

- YAI-5114

  ID-Consumer from Pluggable UI is not migrated to API Gateway.

  The policy ID-Consumer created in older version of CentraSite using Pluggable UI is not migrated correctly to API Gateway when deployed from CentarSite 10.1.

  There is no workaround for this issue.

- YAI-5120

REST Service clients receive response with status code 401 for NTLM authentication in transparent mode.

Though service invocations are successful with NTLM authentication in transparent mode, a response with status code 401 OK is returned.

There is no workaround for this issue.

▪ YAI-5136

API deployment from CentraSite to API Gateway gives exception without alert message.

API deployment from CentraSite to API gateway would fails when APIs are configured with monitoring or throttling policies and no alert message.

To workaround this issue, configure the alert message and deploy the API.

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:

   ▪ 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 10.0

▪ YAI_10.0_Fix5

Release 9.12

▪ YAI_9.12_Fix5

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 10.1

Added Item	Description
Migration from Mediator to API Gateway	APIs and associated data can be published from CentraSite to API Gateway 10.1 version.
	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.

Added Item	Description
Migration from Enterprise Gateway to API Gateway	Enterprise Gateway configurations and Rules can be migrated to API Gateway, which replace and play the role of Enterprise Gateway.
Staging and Promotion support	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. API Gateway assets can be managed with version control system and perform scheduled or automatic promotion to stages as configured.
Support for SOAP over JMS	Support JMS protocol of Inbound and Outbound for SOAP. Allow JMS-HHTP bridging between Inbound and Outbound.
Backup and Restore	Backup API Gateway assets and configuration using command line and you can restore the backed up data.
Transaction based licensing	License model based on transactions and appropriate alerts can be implemented
Approval model for applications	Approval model can be implemented for creating or updating applications, associating applications with APIs, and subscribing to packages.
API Mocking	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.

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.

Added Item	Description
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.
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.

Added Item	Description
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.
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

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-101-20171017