Oracle API Gateway 11.1.2.3.0 Release Notes

Document version: 30 April 2014

New features and enhancements

API Gateway as an OAuth 2.0 client to API Gateway, Salesforce, and Google: API Gateway already provides OAuth 2.0 Authorization Server and Resource Server capabilities to protect REST APIs. In this release API Gateway can be an OAuth 2.0 client to invoke OAuth-protected REST APIs. This enables you to integrate on-premise applications as OAuth clients with cloud applications that expose OAuth-protected REST APIs. A web-based demo client is provided to demonstrate the OAuth client capabilities.

Amazon Web Services (AWS): API Gateway has always been able to connect to Amazon AWS using REST APIs and SOAP web services. In this release API Gateway provides new capabilities for managing Amazon access keys. Amazon access keys are centrally managed in API Gateway, providing improved security and control around accessing Amazon. You can define authorization profiles with the access key obtained from Amazon, and use this profile when connecting to Amazon using the Connect to URL filter.

Amazon Simple Queuing Service (SQS): SQS is Amazon's cloud-hosted messaging system, and API Gateway now provides connectivity with SQS allowing messages to be sent and received. This enables the integration of Amazon SQS with on-premise messaging systems and applications. API Gateway provides a new listener that polls a named SQS queue at set intervals for new messages to be processed, and a new filter that writes messages to SQS queues.

Amazon Simple Storage Service (S3): S3 is an online cloud storage web service offered by Amazon that provides a simple web services interface to store and retrieve data. API Gateway provides filters to upload and download data from S3.

Amazon Simple Notification Service (SNS): SNS is a fully managed push messaging service to push notifications to a range of recipients: directly to mobile devices such as iPhone and Android, SMS text messages, email, Amazon SQS queues, or any HTTP endpoint. In this release API Gateway can send alert messages to Amazon SNS for delivery to the intended recipients.

WebSockets: API Gateway supports the WebSocket protocol, enabling full-duplex asynchronous communication between a client (typically a browser) and a server. WebSockets is used to enhance the interaction between a browser and a web site, facilitating live content and interactive applications such as chat. API Gateway is a WebSocket proxy sitting between the client and the server.

Embedded Apache ActiveMQ: API Gateway is now a native JMS provider by embedding Apache ActiveMQ 5.9. An ActiveMQ broker is embedded in each API Gateway instance, with brokers organized by the API Gateway groups. An active/active deployment is supported, using ActiveMQ's master/slave architecture, to ensure high availability of the messaging infrastructure, with an external shared file system providing the persistent message store. Queue and topic management is integrated into the API Gateway Manager web UI, allowing the API Gateway Administrator to view queues and topics, view messages on queues, and view the contents of individual messages. API Gateway can receive and send messages from and to queues and topics on embedded ActiveMQ using the existing JMS listener and filter.

CORS support: Cross-Origin Resource Sharing (CORS) provides a mechanism for browser-based applications to make requests to a resource in another domain. In API Gateway, HTTP listeners can be configured to support CORS to selectively allow access by web applications running in other domains.

Support for virtual hosts: Virtual hosting is the practice of serving multiple web sites from a single web server. This allows a single API Gateway to appear that it is hosted on several hosts by providing APIs and web services on different virtual hosts. In addition, the API Gateway can host multiple copies of the same API (with the same path and HTTP method) on different virtual hosts. The API Gateway supports *name base* virtual hosting, requiring that the DNS server is configured to map each virtual host name to the correct IP address of the API

Gateway, and the API Gateway is configured to recognize the virtual host names.

Easier SOAP-to-REST: In this release API Gateway provides a number of new features to make exposing SOAP web services as REST APIs easier for the policy developer using Policy Studio:

- Updates to the Validate REST filter to extract parameters into message white board variables make it easier to expose REST APIs with URL-based parameters.
- Enhancements to the Set Message filter make it easier to create the SOAP/XML message to be sent to the target service. You can now generate the message from the WSDL of the target service, and you can graphically insert the parsed REST parameters from the filter into the SOAP message.
- Enhancements to the XML to JSON filter make it easier to convert the SOAP/XML response message to JSON to be returned to the client. You can now remove namespaces and retrieve a subset of the XML message based on an XPath expression.

A "cookbook" detailing step-by-step instructions for exposing SOAP web services as REST APIs using this approach is also available.

Resource repository: API Gateway now has an internal repository for managing multiple versions of imported backend WSDLs and XSDs as they change over their lifecycle and are imported into the API Gateway. API Gateway maintains multiple versions of backend WSDLs and XSDs as they evolve over time and are imported into Policy Studio. As the web service is updated, Policy Studio can resynchronize with it to import new versions of the WSDL and XSDs. API Gateway now prevents invalid WSDLs and XSDs being imported into Policy Studio, and invalid WSDLs and XSDs must be corrected externally before importing. In addition, API Gateway now shares common XSDs that are used by multiple web services rather than duplicating them.

Admin Node Manager High Availability: This release provides an active/active high availability solution for the Admin Node Manager, supporting multiple DMZ deployment patterns. Multiple Admin NMs in a domain are supported in an active/active configuration, with each Admin NM able to perform management operations with topology and configuration shared amongst them.

Configuration locking: This release allows a policy developer to lock a configuration they are editing using Policy Studio, thus preventing other policy developers potentially overwriting their changes. Other

policy developers can download and view the configuration using Policy Studio, but they are prevented from deploying to API Gateway while the configuration is locked. The API Gateway administrator can view which policy developer has the lock, and force a release of the lock if required.

KPS Management UI in API Gateway Manager: This release provides a UI in the API Gateway Manager console to manage the data in the Key Property Store (KPS) by performing create, read, update, and delete (CRUD) operations.

Enhanced certificate management for Node Managers: The enhancements include:

- External CAs can be used to sign SSL certificates for Node Managers and API Gateways as CSRs are now generated.
- The `managedomain` utility can be used as a CA on a locked-down box that runs no domain related processes (it can generate and hold the domain private key and sign CSRs for all Node Managers and API Gateways in the domain).
- Certificate extensions are now used to determine if a Node Manager has administrative capabilities.

Switch filter enhancements: The Switch filter now uses the labels `Equals` and `Does not equal` instead of `Is` and `Isn't` to improve understanding.

Access token cache enhancements: Purging access tokens from the cache now runs in the background.

Policy Studio performance enhancements: Policy Studio now performs better when working with large configurations.

Topology upgrade: In previous versions it was not possible to upgrade your topology. Now, topology upgrade is supported.

Upgrade enhancements: Upgrade now supports configurations with custom listeners.

FTP poller enhancements: The enhancements include:

- When working with a policy used by an FTP poller, the FTP poller context is now shown.
- It is now possible to specify the maximum number of threads when **Establish new session for each file found** is selected.

Default file name for email attachments: The default file name for email attachments is now configurable instead of being set to `attachment.bin`.

User store admin user removed: The user `admin` that existed in the user store in previous versions has been removed, to remove any confusion between this user and the administrative users stored in `adminUsers.json`.

XML to JSON filter enhancements: This filter now has an option to remove namespaces when converting from XML to JSON, as JSON does not have namespaces.

PGP filter enhancements: The PGP filters now support AES256 encryption and decryption.

JSON to XML filter enhancements: This filter now inserts a root element when converting JSON to XML.

OAuth refresh tokens enhancement: OAuth refresh tokens now remain operational until they expire, even if there are requests for access tokens in the interim where a refresh token is not provided.

Oracle Access Manager filter enhancements: This filter now retrieves the OAM headervars.

SMTP filter enhancements: This filter now supports sending the content as the message body and as an attachment.

API Gateway Manager enhancements: You can now start and stop API Gateway instances from the API Gateway Manager web console.

XML to JSON filter enhancements: This filter now supports retrieving a subset of the XML based on an XPath expression.

McAfee Anti-Virus filter enhancements: This filter now requires the McAfee 5600 Scan Engine and a valid McAfee license.

TIBCO EMS client removed: The TIBCO EMS client has been removed. Instead, you can use the JMS client to interact with TIBCO EMS.

Domain audit log enhancements: The enhancements include:

- The deployment, policy, and environment package properties (metadata) are now written to the domain audit log when deploying. This provides an audit of what packages were actually deployed.

- Admin Node Manager operations are now added to the domain audit log.

Database support: API Gateway now supports the following databases:

- MySQL Server 5.1, 5.6
- Microsoft SQL Server 2005, 2008, 2012
- Oracle 11.2, 12.1
- IBM DB2 9.7, 10.5

Messaging system filter enhancements: This filter now supports setting the JMS queue name in the **Destination** field using a selector.

Simplified installation: The API Gateway installer has been simplified to make installing the product easier for both new and advanced users.

Documentation refresh: This release includes a dedicated Administrator Guide detailing all the administrative tasks to deploy and operate the API Gateway in enterprise environments.

Fixed problems

Case ID	Internal ID	Description
D-66625	122479	**Web service WSDL fails during deployment due to namespace in XSD** Previously, the WSDL for a web service could fail to deploy if the schema included other schemas. Now, the WSDL for this web service deploys successfully due to the fact that the API Gateway no longer in-lines included XML schemas before storing them.
—	121570	**Deploying with passphrases not mentioned** Previously, the user documentation did not explain how to deploy passphrase-protected configuration. Now, the *Administrator Guide* and *Deployment and Promotion Guide* include details on deploying and promoting passphrase-encrypted configuration.

Case ID	Internal ID	Description
D-65572	121315	**Failed to execute runnable (org.eclipse.swt.SWTError: No more handles) trying to import policy** Previously, large imports could fail on Windows systems. Now, the overly images associated with diff nodes do not leak, which was causing an issue on Windows systems when importing a large configuration.
—	121209	**User Guide > Utility > Check Group Membership Group field description inaccuracy** Previously, the documentation for the Check Group Membership filter did not reflect the latest fields. Now, the documentation for the Check Group Membership filter is updated to reflect the latest screen. The **Group from Selector Expression** field is also renamed to "Group" because you can enter a string or a selector.
D-65370	121112	**Failed to authenticate via LDAP due to wrong socket factory used in thread** Previously, the wrong socket factory was being used in some threads. Now, the correct socket factory is always instantiated for each thread in the system, removing this intermittent failure.
D-65262	120998	**Import from WSDL option in Schema Cache not working correctly** Previously, the **Import from WSDL** option did not always work correctly. Now, we are using a new internal store for WSDLs and schemas which tracks these resources with greater fidelity, removing problems of this type where documents are transformed incorrectly on import.
D-65118	120855	**upgradeconfig error with Maximum Messages throttling filter in XML Threat Policy coming from 5.2.8 or 6.3.1** Previously, the `upgradeconfig` script set the value

Case ID	Internal ID	Description
		of the field "rate limit based on" to `${${http.request.clientaddr}}` instead of `${http.request.clientaddr.getAddress()}`. Now, the key value is upgraded correctly to `${http.request.clientaddr.getAddress()}`.
D-65038	120754	**Browser left open on admin node port 8090 prevents deployments after certificates reset** Previously, when an SSL-level error occurred during communication with a peer, the API Gateway terminated new unrelated SSL sessions. Now, when an SSL-level error occurs during communication with a peer, the error state is cleaned up correctly. This prevents API Gateway from mistaking a new unrelated SSL session as a failure and terminating this session.
D-64758	120450	**Security issues identified during security audit** Previously, some security issues existed with the API Gateway appliance. Now, the security issues which were raised have been successfully resolved. Some of the issues required changes to the SSH conf file, others involved disabling the SNMP service. Changes were also included in webmin to set HttpOnly on the session cookie, and disable autocomplete in the WAI login page.
D-64733	120420	**Running yum from admin segvs** Previously, running yum as the admin user resulted in segvs. Now, if the admin user runs yum it no longer segvs, but displays an error indicating that yum must be run by the superuser.
D-63246	118878	**Right-clicking on differences in compare and merge tool does nothing** Previously, the ability to filter nodes for viewing differences or for merging was not available. Now, the view nodes and select nodes drop down

Case ID	Internal ID	Description
		menus have been added to the compare and merge tool, allowing the user to select changes.
D-63097	118727	**KPSAdmin: Cannot delete rows with space in them on DB-backed KPS** Previously, you could not delete rows with spaces in them. Now, spaces are handled correctly and the rows can be deleted.
D-63074	118699	**Cannot import WSDL into 7.2.2 that works in 5.2.8** Previously, a WSDL could not be imported into version 7.2.2 that was imported successfully in version 5.2.8. Now, the WSDL can be imported when it is changed to be WSI-compliant with respect to R2001.
D-62744	118360	**Elements of type "import" cannot appear after declarations** Previously, a WSDL could not be imported if it contained imports after declarations. Now, we are using a new internal store for WSDLs and schemas which tracks these resources with greater fidelity, removing problems of this type where documents are transformed incorrectly on import.
D-62743	118359	**Incompatible attribute found for include: {null}version** Previously, you could not register a web service that used a WSDL and XSD files with different version attributes. Now, we are using a new internal store for WSDLs and schemas which tracks these resources with greater fidelity, removing problems of this type where documents are transformed incorrectly on import.
D-62562	118162	**Crash when "Record payload data received" option on a HTTP interface is disabled** Previously, disabling an option on the **Traffic**

Case ID	Internal ID	Description
		Monitor tab of a HTTP interface could result in a crash. Now, selecting or deselecting all options when configuring the HTTP interface does not cause a crash.
D-60389	116684	**Clean up ORACLE JDBC jar (KPS using DB for storage cannot store many long redirect URLs)** Previously, registering OAuth client applications with several long redirect URLs resulted in errors when using a Oracle database for KPS. Now, API Gateway ships with a jar which fixes this issue (`ojdbc6.jar`).
D-60272	116539	**Renaming HTTP interface not reflecting in Policy Studio until after deploy** Previously, renaming an HTTP interface in Policy Studio did not always take effect until the configuration was deployed. Now, renaming an HTTP interface takes effect immediately.
D-60018	116168	**Apache Access File Logger uses wrong file format** Previously, the difference between the deprecated Access Log filter and new path-based Apache access file logging was not clear. Now, the deprecated Access Log filter has been removed, and the documentation has been updated to reflect this change.
D-59118	115214	**JMS multiple threads issue** Previously, session threads were not being reused successfully. Now, JMS Tibco session threads are reused successfully.
D-55655	112049	**Adding Amazon Commerce WSDL fails with an error message** Previously, WSDL containing the same operation on multiple ports failed to import.

Case ID	Internal ID	Description
		Now, the import dialog in Policy Studio guards against reimporting the same binding operation more than once.
D-53886	109811	**Embedded schemas with no targetNamespace or an empty import statement fail to import** Previously, the WSDL for a web service could fail to import if it included an embedded schema with no targetNamespace or an empty import statement. Now, due to an upgrade of the internal schema validation engine, this WSDL is imported successfully.
D-53437	109322	**WSDL endpoint changed if web service name is changed** Previously, the `soap:address location` of a WSDL was reset to its original (non-virtualized) value if the web service name was changed in Policy Studio. Now, the endpoint name is consistent with that of the virtualizing gateway, as expected.
D-52010	109084	**WSDL with multiple service ports for same binding causes errors** Previously, a WSDL that contained multiple service ports for the same binding failed to import. Now, the import dialog in Policy Studio guards against reimporting the same binding operation more than once.
D-51991	109063	**Global request policy not used in calculating attributes being set** Previously, attributes set during the execution of the global request policy were not available to other policies. Now, if an attribute is set during the execution of the global request policy, this attribute is available subsequently to other policies.
D-51973	109045	**KPS REST API returns 201 error on POST and PUT.**

Case ID	Internal ID	Description
		Previously, the KPS REST API returned an error on POST and PUT. Now, the KPS REST API returns 201 Create on POST and PUT.
D-51969	109041	**Error in response service handler when client leg uses encryption** Previously, an error `Can't find Handler for operation` was generated when encryption was used. Now, the web service handler can successfully resolve encrypted response messages in policies that have been autogenerated from a WS-Policy.
D-51957	109029	**Import from WSDL option in Schema Cache not working correctly** Previously, some schemas that referenced other schemas could not be imported correctly. Now, we are using a new internal store for WSDLs and schemas which tracks these resources with greater fidelity, removing problems of this type where documents are transformed incorrectly on import.

Back to Top

Known issues

The following are known issues with this version of API Gateway:

KPS browser

- It is not possible to add a new row in the KPS browser when the row has autogenerated or encrypted columns.
- If KPS changes are made via KPS admin then the KPS browser must be reloaded before the changes are visible.

OAuth client

- If an OAuth token expires then the OAuth sample client must be refreshed in the browser.

Topology

- If you are running with more than one ANM and you want to make topology changes then all ANMs should be able to communicate with each other to ensure consistency of topology.
- If topology changes are made outside of a browser then the browser must be refreshed to pick up the latest changes.
- Two ANMs trying to push topology updates at the same time can lead to both ANM's Topology APIs being locked until a connection timeout occurs.

Miscellaneous

- When running two instances on the same machine which belong to the same group you must make sure that each instance uses a different IP address in the cassandra.yaml file. Alternatively, one of the instances should be be marked as a Cassandra client by deleting the cassndra.yaml file.
- In Policy Studio, client credentials do not automatically update in the navigation tree if they are added outside of the navigation tree.

Back to Top

Related documentation

Oracle API Gateway is accompanied by a complete set of documentation, covering all aspects of using the product. These documents include the following:

Oracle API Gateway documentation

- Oracle API Gateway Concepts Guide
- Oracle API Gateway Installation and Configuration Guide
- Oracle API Gateway User Guide
- Oracle API Gateway Administrator Guide
- Oracle API Gateway Deployment and Promotion Guide

- Oracle API Gateway OAuth User Guide

Support Services

When you contact Oracle Support with a problem, be prepared to provide the following information for more efficient service:

- Product version and build number
- Database type and version
- Operating system type and version
- Description of the sequence of actions and events that led to the problem
- Symptoms of the problem
- Text of any error or warning messages
- Description of any attempts you have made to fix the problem and the results

You can display the version and build of API Gateway by selecting **Help > About** in Policy Studio.

Back to Top
