Oracle API Gateway 11.1.2.4.0 Release Notes

Document version: 29 October 2015

- New features and enhancements
- Fixed problems
- Known issues

  ALERT: See the Known Issues section for important post-install steps you must complete to run Oracle API Gateway on Solaris.

- Documentation
- Support services

New features and enhancements

The following new features and enhancements are available in this release.

Security

- FIPS-140-2 and NIST Suite B compliance – API Gateway includes a new tool that can inspect your configuration against FIPS, SuiteB, and SuiteB Top Secret security requirements, and that lists everything that does not conform to the selected profile.
- API firewalling – API Gateway embeds Apache ModSecurity; a toolkit for real-time HTTP traffic monitoring, logging, and access control; to help companies mitigating application-level threats on their APIs. When threat protection is enabled, all traffic is processed by the ModSecurity engine, based on the configured threat protection rules. You can write your own rule sets, or you can use one of the several free and paying rule sets provided by specialized vendors. ModSecurity activity is visible and can be filtered from the Traffic view in API Gateway Manager.
- SafeNet Luna HSM integration – You can now configure an API Gateway instance to interoperate with a Safenet Luna SA HSM device and seamlessly map objects stored in the device to API Gateway encryption and signing capabilities. The object segmentation used in the Luna devices (slots) is abstracted in the API Gateway through the use of certificate realms and the certificate store allowing security architects to hide complexity from policy developers and decouple secure key storage from policy development.This feature supports only RSA keys.

Enterprise messaging

- Predefined JMS services – API Gateway now comes with predefined settings for the embedded ActiveMQ, external ActiveMQ and external IBM MQ cases. The corresponding JAR files are also now delivered out-of-the-box.
- JMS SSL/TLS settings – The JMS security configuration is now integrated in the Entity Store and relies on its certificate and key store. This enables you to select the cipher suites, trusted certificates, and client certificate used, and to leverage an HSM when appropriate.
- Automatic reconnection – API Gateway now adds a supplemental layer on top of the automatic reconnection feature natively provided by JMS providers, to handle reconnection when the JMS layer does not fulfill its mission properly.
- Message removal policy – When implementing a JMS listener you can now choose from four different message removal policies:
    - remove immediately when read
    - remove lazily and allow duplicates
    - remove when policy completes without error
    - remove when policy completes and the value of a property evaluated at the end of the policy execution is true
- Durable subscribers – You can now configure a durable subscription to JMS topics.
- Read from JMS filter – This new filter can read JMS messages from within a policy flow. It is as an alternative to the JMS Listener which is continuously reading new messages arriving on queues. This filter can block and wait for messages from 1ms to 20s. Accordingly, the Messaging System filter (writing to the queues/topics) has been renamed as Send to JMS.

For more information on enterprise messaging, see the *API Gateway Policy Developer Guide*.

Logging and analytics

- Logging of transaction event data to file – API Gateway now supports writing individual transaction event data, including custom fields, to a local transaction event log file in JSON format.
- The local Node Manager reads this file, aggregates the metrics data, and writes it to the API Gateway Analytics database using JDBC. Previously each API Gateway wrote the metrics data to the Analytics database directly using JDBC. If the database was not available then the data would not be recorded, potentially leading to the loss of metrics data. Now, if the database is not available the transaction event data will continue to be written to the local log file and the metrics data will be uploaded when the database becomes available.
- In addition, this enables easy integration with third party reporting, analytics, and billing systems as the transaction event data in the log file can be read and uploaded.

- Eliminate transaction performance impact of logging – All file-based logging is now performed independently of any thread executing an API request. This includes logging data to the Traffic Monitor log, transaction audit log, transaction data log, and trace log. This means you can enable logging without any impact to the performance of the API Gateway executing requests. This enhancement also ensures that all requests will have a consistent SLA performance.

For more information on logging and analytics, see the *API Gateway Administrator Guide*.

Back to Top

Fixed problems

Bug ID	Description
—	**Issue:** API Gateway could crash due to out of memory error caused by memory leaks while handling connection input/output exceptions. **Resolution:** API Gateway deallocates all memory when handling connection input/output exceptions.
—	**Issue:** System backup for appliances did not report errors when backup process failed. **Resolution:** System backup for appliances now reports errors if the backup process fails.
—	**Issue:** Previously, API Gateway used version 5600 of the McAfee Anti-Malware Engine. **Resolution:** Now, it uses version 5700 of the McAfee Anti-Malware Engine.
—	**Issue:** Previously, you were unable to connect to a URL using an API Gateway configured as an HTTPS proxy. **Resolution:** Now, you can connect to a URL using an API Gateway configured as an HTTPS proxy.
18815229	**Issue:** Previously, the CRL filters were validating certificates using expired CRL from cache. **Resolution:** Now, the CRL filters return false if the provided/cached CRL is expired.
—	**Issue:** Previously, there was an issue with upgrading XML files with

Bug ID	Description
	UTF-8 encoding. **Resolution:** Now, there is no issue with upgrading XML files with UTF-8 encoding.
—	**Issue:** Previously, the support for Solaris 64 bit was documented incorrectly. **Resolution:** Now, the support for Solaris 64 bit is documented correctly.
—	**Issue:** Previously, the Trace filter was terminating API Gateway processing a UTF-8 encoded character. **Resolution:** Now, the Trace filter is fixed to allow processing a UTF-8 encoded character.
—	**Issue:** Previously, you were unable to connect to an HTTPS URL through an HTTP/HTTPS proxy. **Resolution:** Now, it is possible to connect to an HTTPS URL through an HTTP/HTTPS proxy.
19387262	**Issue:** Previously, when registering WSDL using WSDL URL, API Gateway always sent an authentication header to the remote server, disregarding authentication settings. **Resolution:** Now, when registering WSDL using WSDL URL, API Gateway sends the authentication header only if the authentication settings are provided.
19404204	**Issue:** Previously, SAML Attribute Assertion filter throws an error under heavy load. **Resolution:** Now, SAML Attribute Assertion filter does not throw an error under heavy load.
—	**Issue:** Previously, when using REST API wizards to create an API in Policy Studio, the parameter path variables were not available on the whiteboard for the Request/Routing/Response policies. **Resolution:** Now, when using REST API wizards to create an API in Policy Studio, the parameter path variables are available on the whiteboard for the Request/Routing/Response policies.
—	**Issue:** Previously, API Gateway was not always sending close-notify message on SSL shutdown. **Resolution:** Now, API Gateway sends close-notify explicitly on SSL

Bug ID	Description
	shutdown. You can configure this in SystemSettings of API Gateway instance's service.xml config: `sslShutdownPolicy = {"dirty" | "simplex" | "duplex"}` • "dirty" is the old behaviour • "simplex" is the default, and ensures that close-notify is sent • "duplex" waits for the remote to send its close-notify also
19482339	**Issue:** Previously, the User Guide did not document which JSON Schema specifications are supported by the JSON Schema Validation filter. **Resolution:** Now, draft version 2 of JSON Schema specification supported by the JSON Schema Validation filter is added in the Policy Developer Guide.
—	**Issue:** Previously, there were errors when managedomain was creating a Node Manager because of permissions on the system. **Resolution:** Now, there are no errors when managedomain creates a Node Manager.
—	**Issue:** Previously, INVALID_FIELD was returned for an invalid field in selectors in policies. **Resolution:** Now, there is a configuration option to allow an empty string to be returned instead of the INVALID_FIELD value from selectors.
—	**Issue:** Previously, the Connect to URL filter always added the port number in Host header for HTTP and HTTPS requests (for example, Host: www.oracle.com:80, Host: www.oracle.com:443). **Resolution:** Now, the Connect to URL filter adds only non-default ports for HTTP and HTTPS requests in the Host header (for example, Host: www.oracle.com).
—	**Issue:** Previously, in certain circumstances the XML parser allowed DTD injection when parsing SOAP XML documents. **Resolution:** Now, it is not possible to inject DTDs into XML because the XML parser does not allow it.
—	**Issue:** Previously, Policy Studio could not connect to an Admin Node Manager configured for TLS 1.2. **Resolution:** Now, you can use a configuration option in policy.ini to

Bug ID	Description
	connect to an Admin Node Manager configured with TLS 1.2 using Policy Studio.
19631828	**Issue:** Previously, under certain conditions when importing a policy, the policy did not import correctly and was missing links. **Resolution:** Now, when importing the policy, all links are properly imported.
—	**Issue:** Previously, the Connect to URL filter was sending CONNECT method with endpoint set to proxy. **Resolution:** Now, the Connect to URL filter sends CONNECT method to proxy with correct endpoint details.
—	**Issue:** Previously, using basic authentication with "Automatically send credentials" enabled, the API Gateway crashed. **Resolution:** Now, using basic authentication with "Automatically send credentials" enabled, the authentication process completes.
—	**Issue:** Previously, OAM Authenticator returned a fatal error when it cannot find a scoped session during authentication. **Resolution:** Now, OAM Authenticator no longer returns a fatal error if it cannot find the scoped session.
—	**Issue:** Previously, harmless messages appeared in trace log file for licensing. **Resolution:** Now, these messages have been removed from the trace log file because they are not useful.
—	**Issue:** Previously, the API Gateway Node Manager reported an error when users attempted to download a trace file exceeding 10 MB in size. **Resolution:** Now, you can configure the API Gateway Node Manager using the samples/scripts/config/updateMaxInOutLen.py script to allow downloading a trace file exceeding 10 MB in size.
—	**Issue:** Previously, some operations were not listed when registering WSDL in Policy Studio. **Resolution:** Now, all operations are listed when registering WSDL in Policy Studio.
—	**Issue:** Previously, API Gateway was running with an older version of OpenSSL.

Bug ID	Description
	Resolution: Now, API Gateway is running with OpenSSL 1.0.1j 15 Oct 2014.
—	**Issue:** Previously, the disable Cassandra script did not allow you to specify an Admin Node Manager URL. **Resolution:** Now, the disable Cassandra script allows you to specify an Admin Node Manager script.
—	**Issue:** Previously, WSDL with space in namespace name could not be loaded. **Resolution:** Now, validation of namespaces can be turned off using the new XML_PARSE_NONAMESPACE_URI_REF_VALIDATION libxml custom option to allow loading WSDL with space in namespace name.
—	**Issue:** Previously, the API Gateway Node Manager reported an error when users attempted to download a log file exceeding 10 MB in size. **Resolution:** Now, you can configure the API Gateway Node Manager using samples/scripts/config/updateMaxInOutLen.py script to allow downloading a log file exceeding 10 MB in size.
20023344	**Issue:** Previously, under certain circumstances, there was a race condition when processing XPath expressions. **Resolution:** Now, there is no race condition when processing XPath expressions.
20048725	**Issue:** Previously, when the Directory Scanner was dealing with large files, it read the whole file into memory causing an OutOfMemoryException. **Resolution:** Now, the Directory Scanner does not read the whole file into memory, and does not cause any OutOfMemoryExceptions.
20049128	**Issue:** Previously, API Gateway crashed using an ICAP filter because of a connection input/ouput error sending content to ICAP server. **Resolution:** Now, API Gateway correctly handles the connection input/output error while sending content to ICAP server.
—	**Issue:** Previously, the FTP poller failed to delete processed files (if configured) from the FTP server because of a connection error. **Resolution:** Now, the FTP poller retries to delete processed files from the FTP server on connection error.

Bug ID	Description
—	**Issue:** Previously, the CRL (Dynamic) filter failed to resolve selector with generated legacy message attributes, for example: `${distributionpoint.0.1.toString}, ${distributionpoint.0.0.toString}` **Resolution:** Now, the CRL (Dynamic) filter resolves selector with generated legacy message attributes.
—	**Issue:** Previously, the McAfee Anti-Virus filter could crash scanning message body or cause a memory leak. **Resolution:** Now, the McAfee Anti-Virus filter cleans up temporary allocated memory.
—	**Issue:** Previously, the Sentinel server external connection was always configured with the provided encoding. **Resolution:** Now, the Sentinel server external connection applies the provided encoding only if the IGNORE_ENCODING Java property value is false (default).
—	**Issue:** Previously, the Throttling filter was setting duplicated Throttling rate limit information headers in the response. **Resolution:** Now, the Throttling filter sets Throttling rate limit information headers in the response once.
20202027	**Issue:** Previously, the Threatening Content filter was not trapping content that is not escaped. **Resolution:** Now, the Threatening Content filter is trapping content that is not escaped.
—	**Issue:** Previously, the McAfee Anti-Virus filter may not always correctly update the 'mcafee.status' message attribute for multipart messages. **Resolution:** Now, the McAfee Anti-Virus filter merges scan results into the 'mcafee.status' message attribute for multipart messages.
—	**Issue:** Previously, the Connect to URL filter was unable to connect to a URL via an HTTPS proxy. **Resolution:** Now, it is possible to connect to a URL via an HTTPS proxy.
—	**Issue:** Previously, in OAuth the redirect URL was seen as invalid because the host was a different case to the one stored on disk for the profile.

Bug ID	Description
	Resolution: Now, there is no longer case sensitivity on the host part of the redirect URL.
—	**Issue:** Previously, a false error was reported for recursion in a specific policy when using policy shortcuts. **Resolution:** Now, there is no error reported for the specific policy using policy shortcuts because it is a valid policy.
—	**Issue:** Previously, there was a problem with case sensitivity in URL parameters. **Resolution:** Now, you can configure API Gateway to use case sensitive or case insensitive values for URL parameters.

Back to Top

Known issues

The following are known issues in this version of API Gateway.

Solaris

ALERT: You MUST perform the workarounds described in this section after installation for Oracle API Gateway to run on Solaris. You do not have to complete these workarounds on Linux or Windows systems.

- Execute rights are missing in various binaries for Policy Studio and Configuration Studio on Solaris.

  Workaround: Execute the following command on the Policy Studio and Configuration Studio directories:

  ```
  chmod -R u+x *; chmod  u+x .launch
  ```

- Policy Studio and Configuration Studio will not start and the trace file reports the following Java exception:

  ```
  org.eclipse.swt.SWTException: Unable to load
  graphics library [Cairo is required]
  ```

  Workaround: Execute the following command:

  bash/ksh:

  ```
  export LD_LIBRARY_PATH=/usr/lib/gnome-
  private/lib/
  ```

csh:

```
setenv LD_LIBRARY_PATH /usr/lib/gnome-private/lib/
```

Documentation

- The PDF version of the Oracle API Gateway Developer Guide states that the Oracle API Gateway REST API reference documentation is available in the following directory after installing the product: `INSTALL_DIR/apigateway/docs/restapi`. The Oracle API Gateway REST API Reference document is not available in this directory. You can find the REST API Reference document at http://docs.oracle.com/cd/E65459_01/apirefs.1112/e65673/index.html.

Topology

- If you are running with more than one Admin Node Manager and you want to make topology changes then all Admin Node Managers 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 Admin Node Managers trying to push topology updates at the same time can lead to both Admin Node Manager's Topology APIs being locked until a connection timeout occurs.

Upgrade

- When upgrading from previous version of a configuration that contains OAuth services it will be necessary to run the deploy script again, for example:

```
./run.sh oauth/deployOAuthConfig.py --importapps=off
```

- This will overwrite the OAuth 2.0 Services HTTP Listener, so if the existing configuration has to be kept, the OAuth 2.0 Services HTTP Listener should be renamed before running the script.

Redaction

- If redaction is required in the context of XML payloads where data can be sent by the client in separate chunks (long documents or slow connections), it is recommended to utilize raw redaction (regular expression-based) as opposed to XML redaction configuration.

API firewalling

- API firewalling capability is not available on Windows and Solaris platforms.
- On some Linux platforms, when traffic matches an API firewalling (ModSecurity) rule containing a “deny” action, the client connection might be dropped.
- API firewalling (ModSecurity) rules containing a “block” action fail to fall back to the configured SecDefaultAction, instead resuming normal processing. The use of “deny” action is recommended in those cases.
- API firewalling (ModSecurity) rules operating on phases 3 and 4 (response headers and body processing) are not supported. These rules will have no effect on API Gateway behavior.

OEM plugin

- OEM plugin does not show graphs for Service Usage per Client data. It will show graphs for Service Usage per Method data instead with incorrect labels.

OAuth

Internet Explorer issues in the OAuth UI and OAuth client demo:

- JavaScript error on line 47 of Authorization form when clicking on the Allow button. Error in `${VDISTDIR}install/samples/oauth/templates/requestAccess.html`. To fix the error, remove `onclick="formSubmit();"`.
- Typo in the first character of the OAuth client demo `${VDISTDIR}install/samples/oauth/clientdemo/home/index.html` causes display issues in Internet Explorer in compatibility mode. To fix the issue, delete `'f'` at the start of the file.

Back to Top

Documentation

This section describes documentation enhancements and related documentation.

Documentation enhancements

- *Oracle API Gateway Key Property Store User Guide* – New guide describing how to configure and manage the API Gateway Key Property Store (KPS).

- *Oracle API Gateway Policy Developer Guide* – This guide was previously known as the API Gateway User Guide. This guide has been renamed to the API Gateway Policy Developer Guide and is aimed at policy developers using Policy Studio.

For other documentation changes and enhancements, see the "What's new" section in each guide.

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 Administrator Guide*
- *Oracle API Gateway Concepts Guide*
- *Oracle API Gateway Deployment and Promotion Guide*
- *Oracle API Gateway Developer Guide*
- *Oracle API Gateway Installation Guide*
- *Oracle API Gateway Key Property Store User Guide*
- *Oracle API Gateway OAuth User Guide*
- *Oracle API Gateway Policy Developer Guide*
- *Oracle API Gateway User Guide*

Back to Top

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