Axway API Gateway 7.4.1 Release Notes

Document version: 07 August 2015

New features and enhancements

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

Operating system support

Support has been added for following operating systems:

- SUSE Linux Enterprise Server 12 64-bit
- Red Hat Enterprise Linux 7 64-bit
- Oracle Linux 7 64-bit
- Centos 7 64-bit

Support has been removed for the following operating systems:

- Linux 32-bit
- Solaris 32-bit (Solaris 64-bit will be supported in a future release)
- Debian
- Ubuntu

For more information, see the *API Gateway Installation Guide*.

Security enhancments

- Domain audit logs – You can now configure the set of domain audit events that get audited in the domain audit log in API Gateway Manager. You can also periodically offload domain audit logs to an external audit server.

- Password policies – In API Gateway Manager you can now configure password policies for administrator users.
- API firewalling – API firewalling is now supported on Linux and Windows platforms, and has been enhanced with threat protection profiles, which enable you to easily configure threat protection rules and execute policies when a rule is triggered.

For more information, see the *API Gateway Administrator Guide* and the *API Gateway Security Guide*.

Filter enhancements

- JSON Schema Validation filter – This filter now supports v3 and v4 JSON Schema validation.
- Scripting Language filter – This filter now supports JavaScript based on the Nashorn JavaScript engine (JRE8) in addition to JavaScript based on the Rhino JavaScript engine (JRE7 and earlier).
- HTML Form based Authentication filter – This filter has been enhanced to support settings for invalid login attempts.

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

Fixed problems

Case ID	Internal ID	Description
764939	144778, 148021, 148022	**Issue:** Previously, in Policy Studio, the Maximum Sent/Received Bytes per transaction configuration in System Settings were incorrectly set. **Resolution:** Now, the Maximum Sent/Received Bytes per transaction labels in Policy Studio match the actual values set in the configuration.

Case ID	Internal ID	Description
764376	142550, 147872	**Issue:** Previously, a user could specify a P12 file to sign SSL certificates for management traffic that did not contain a full certificate chain (option 2 for cert management). This led to a failure to start the API Gateway due to missing certs in the chain. If the user supplies a p12 with an intermediate CA and a root CA, the trusted CA cert on the SSL ports for Node Manager was the Root CA. **Resolution:** Now, managedomain validates the P12 specified by the user and ensures that the full certificate chain is included (option 2 for cert management). Self-signed certificates are allowed (option 2 for cert management). If the user supplies a p12 with an intermediate CA and a root CA, the trusted CA cert on the SSL ports for Node Manager is now the Intermediate CA, as this is the "Domain CA". Validation on the certificate PEM files submitted for option 3 (External CA) for cert management has also been improved to ensure the full cert chain is included.
772099	146387, 147031	**Issue:** Previously, the API Gateway could crash attempting to log libxml error messages containing %-encoded characters. **Resolution:** Now, the API Gateway logs libxml error messages containing %-encoded characters.
770553	145658, 145986, 146073	**Issue:** Previously, the HTTP Response header had a duplicate Content-Type field when using the ICAP filter. **Resolution:** Now, the HTTP Response header correctly has a single Content-Type field when using the ICAP filter. In the case of a multipart response where the content types are different, multiple Content-Types are still permitted.
—	147361, 147363	**Issue:** Previously, the API Gateway Analytics reports were incorrectly rescheduled on refresh and failed to run. **Resolution:** Now, the API Gateway Analytics reports are scheduled on refresh as expected.
776810	148194, 148186	**Issue:** Previously, the Directory Scanner was also processing folders when no file type was specified in the configuration. **Resolution:** Now, the Directory Scanner processes files as required when no file type is specified in the configuration.

Case ID	Internal ID	Description
772935	146725	**Issue:** Previously, in Policy Studio, a `WebServicePlugin: java.lang.NullPointerException` error was shown when attempting to edit a WebService path in Listeners. **Resolution:** Now, the WebService path can be modified in Listeners with the Web Service Resolver configuration dialog in Policy Studio.
770305	145334, 147549	**Issue:** Previously, the API Gateway was inconsistently crashing when attempting to send a response after processing a large payload when the client had already closed the connection. **Resolution:** Now, the API Gateway reports closed connections as expected when attempting to send a response.
—	147588	**Issue:** Previously, the SAML Attribute Assertion filter was throwing an error under heavy load. **Resolution:** Now, the SAML Attribute Assertion filter does not throw an error under heavy load.
—	147587	**Issue:** Previously, INVALID_FIELD was being 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.
—	147586	**Issue:** Previously, in certain circumstances the XML Parser allowed DTD injection when parsing SOAP XML documents. **Resolution:** Now, it is no longer possible to inject DTDs into XML as the XML Parser will not allow it.
—	147584	**Issue:** Previously, the Connect to URL filter was setting the proxy host name in the Host header instead of the destination host name when sending a request via a proxy. **Resolution:** Now, the Connect to URL filter sets the destination host name in the Host header when sending a request via a proxy.

Case ID	Internal ID	Description
—	147583	**Issue:** Previously, the /metrics call always reported `cpuUsed` as zero. **Resolution:** Now, the /metrics call always shows a positive number in `cpuUsed`.
—	147581	**Issue:** Previously, the File Upload filter always used FTPS settings and ignored FTP settings for ASCII/Binary transfer. **Resolution:** Now, the File Upload filter uses FTPS, FTP, or SFTP configuration settings respectively.
—	147580	**Issue:** Previously, if an API Gateway configuration was protected with a passphrase, a user password in the Proxy settings was not decrypted causing the Proxy-Authorization HTTP header to contain an incorrect value. **Resolution:** Now, a user password in the Proxy settings is correctly decrypted when loading from a passphrase-protected API Gateway configuration.
—	147579	**Issue:** Previously, the Trace filter was terminating API Gateway when processing a UTF-8 encoded character. **Resolution:** Now, the Trace filter is fixed to allow processing a UTF-8 encoded character.
—	147576	**Issue:** Previously, API Gateway Analytics could generate a blank report due to the default timeout (30000 ms) in JavaScript waiting for a generated report. **Resolution:** Now, API Gateway Analytics can be configured with a custom JavaScript timeout using the `javascriptDelay` Java system property in `jvm.xml`, for example, `<VMArg name="-DjavascriptDelay=3600000" />`. The default timeout is now set to 300000 ms.
—	147582	**Issue:** Previously, the API Gateway was crashing if incorrect DH parameters were configured for an HTTPS port listener. **Resolution:** Now, the API Gateway reports incorrect DH parameters supplied for an HTTPS port listener.

Case ID	Internal ID	Description
747264	134130	**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.
765969	143282	**Issue:** Previously, the HTTP Basic filter did not always authenticate a user correctly via a database repository configured to hash a client password. **Resolution:** Now, API Gateway always hashes the client password if configured in the database repository.
—	148739	**Issue:** Previously, a NPE was returned from the Retrieve from or write to database filter when a stored procedure was called that returned a NULL. **Resolution:** Now, when a NULL is returned by the stored procedure it is ignored (no message attribute is set). It is possible to set a blank ("") value in a message attribute for the returned NULL value of the stored procedure by setting the Java system property `ALLOW_NULL_VALUES_FROM_DB=true` in `jvm.xml`, for example, `<VMArg name="-DALLOW_NULL_VALUES_FROM_DB=true" />`.
774947	147941	**Issue:** Previously, if you tried to submit an externally signed cert that did not match the private key on disk you saw an error `java.lang.Exception: java.lang.Exception: RSA_private_decrypt failed`. **Resolution:** Now, you will see `Error: Public key in certificate and private key on disk do not match. Detail: java.lang.Exception: RSA_private_decrypt failed`. **Issue:** Previously, if you submitted a PEM file that did not contain the certificates ordered correctly, for example, NM/GW, followed by Inter CA followed by Root CA you would see the error `TypeError: 'NoneType' object is unsubscriptable`. **Resolution:** Now, if you submit a PEM file that does not contain the certificates ordered correctly they are ordered automatically for you. The order of the certs in the PEM file should not matter.

Case ID	Internal ID	Description
—	147461	**Issue:** Previously, when using `--sign_with_external_ca` and submitting the cert for the first Admin Node Manager, administrator credentials are required and an attempt is made to validate them, but there is no Admin Node Manager running, so cert submission fails. Administrator credentials were also always required for certificate regeneration which might need to be run offline. **Resolution:** Now, credentials are not required when you submit the cert for the first Admin Node Manager. For cert regeneration administrator credentials are only prompted for when and if they are needed, for example, when the Admin Node Manager needs to sign certs for second and subsequent hosts. Credentials are not prompted for on cert submission after cert regeneration with the `--sign_with_external_ca` option.
773131	146938	**Issue:** Previously, the Read Application filter did not add the custom attributes defined in `app.config` to the message attribute that it generates (`apimgmt.application`). **Resolution:** Now, all custom attributes are added to `apimgmt.application`.
—	148742	**Issue:** Previously, if an FTP poller was configured to move the file to a multilevel directory that did not exist, a failure would occur with some SFTP servers as it would not allow the creation of multiple levels of directories via one command. Also some FTP servers would throw errors if the FTP poller tried to create a directory that already existed. It was difficult to diagnose the issue as the SFTP errors were not written to the trace. **Resolution:** Now, the FTP poller will not try to create a directory that already exists. It will attempt to create a directory that does not exist as entered by the user. Some SFTP servers will fail to create a multiple level directory. If a directory cannot be created by the FTP poller it should be done manually. The API Gateway now outputs the SFTP errors to the trace.

Case ID	Internal ID	Description
—	149019	**Issue:** Previously, in Policy Studio, you could not modify the Create Cookie filter of a successfully imported configuration. **Resolution:** Now, in Policy Studio, the Create Cookie filter of a successfully imported configuration can be modified.
—	148847	**Issue:** Previously, some API Gateway shared libraries were using built-in RPATH first searching for other libraries to resolve dependencies. This caused problems loading API Gateway where the built-in RPATH was accidentally matching system paths in a customer's environment. **Resolution:** Now, the RPATH is removed from reported API Gateway shared libraries.
—	148228	**Issue:** Previously, the XML Sign/Verify process was always validating the XML namespaces disregarding the namespace validation flag settings in the LibXml2 configuration. **Resolution:** Now, the XML Sign/Verify process checks the namespace validation flag settings in the LibXml2 configuration.
775794	148652	**Issue:** Previously, the API Gateway was replacing empty XML elements <a> with empty tag <a/>. **Resolution:** Now, the API Gateway provides LibXml2 option to allow generating empty XML element <a> instead of empty tag <a/>.
—	145781	**Issue:** Previously, when using Policy Studio to test an LDAPS connection over SSL, the connection test failed and the exception trace indicated `Unconnected sockets not implemented`. **Resolution:** Now, the connection test to an LDAPS server over SSL no longer generates the `Unconnected sockets not implemented` exception.
777877	148523	**Issue:** Previously, the API Gateway Node Manager could hang on startup due to an AMI license check. **Resolution:** Now, the API Gateway Node Manager uses a default 5000 ms timeout attempting the AMI license check. You can use the `V_AMI_TIMEOUT` environmental variable to set a custom timeout instead of the default.

Case ID	Internal ID	Description
—	146903	**Issue:** Previously, upgrade of a Web Service configuration could fail if the WSDL URL in the Web Service was not normalized. **Resolution:** Now, a Web Service with a WSDL URL that is not normalized is upgraded successfully.
765489	143423	**Issue:** Previously, the system backup for appliances was not reporting errors if the backup process failed. **Resolution:** Now, the system backup for appliances reports errors if the backup process fails.
776969	148208	**Issue:** Previously, examples in the "Example selector expressions" section of the *API Gateway Developer Guide* were using deprecated functions and contained a malformed JSON sample. **Resolution:** Now, examples in the "Example selector expressions" section of the *API Gateway Developer Guide* are corrected.
717206	120910	**Issue:** Previously, CTE was removed from multipart/related bodies. **Resolution:** Now, CTE is kept if an XMLBody of content type `application/xop+xml` including `xop:Include` elements is found in a multipart/related body.
	145282	**Issue:** Previously, Access Log formats were not behaving as documented. **Resolution:** Now, Access Log formats behave as documented.
769579	145412	**Issue:** Previously, the `addCert.py` script deleted the old certificate's details from the entity store. **Resolution:** Now, the `addCert.py` script checks if a certificate with the same alias already exists and updates the entity store with new certificate content. As the certificate is not deleted, the references to HTTPS interfaces are also preserved.

Case ID	Internal ID	Description
760926	142602	**Issue:** Previously, the API Gateway was logging incorrect payload content and URI for outbound connections configured in the Connect to URL filter. **Resolution:** Now, the API Gateway logs outbound connections with content and URI configured in the Connect to URL filter.
769603	144981	**Issue:** Previously, if a Connect to URL filter was invoked, the output variable `http.response.time` was not created. **Resolution:** Now, when a Connect to URL filter is invoked, the output variable `http.response.time` contains the number of milliseconds taken to invoke the URL, for example, `96 ms`.
767641	144496	**Issue:** Previously, the Remove HTTP headers filter was throwing a NullPointerException trying to access the missing `http.headers` attribute. **Resolution:** Now, the Remove HTTP headers filter processes `http.headers` attributes if present.

Known issues

The following are known issues for this release of API Gateway.

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 version 7.1.0, exporting from 7.1.0 might cause an error in KPS. If that occurs, create the file `apiserver/conf/jvm.xml` with the following contents:

```
<ConfigurationFragment>
<ClassDir name="$VDISTDIR/upgrade/legacy/7.1.x/" />
</ConfigurationFragment>
```

- 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.

- When upgrading from version 7.4.0, you might also need to set the class for any custom OAuth 2.0 providers before upgrading. For more information, see *OAuth provider upgrade* on page 12.

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.

OEM plug-in

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

FIPS mode

- When running an API Gateway instance in FIPS mode, the following features will produce non-compliant behaviors:
  - Connectivity to Axway PassPort.
  - Connectivity to RSA Access Manager.
  - ECDSA-based encryption, decryption, signing, and verification operations.
- When enabling FIPS mode on Windows platforms via the `togglefips.bat` command, although the command completes successfully, the necessary changes in the environment will not be applied. Contact Axway Support if you need to enable FIPS mode on Windows platforms.

Axway PassPort

- If there are multiple PassPort authentication repositories defined and there are issues connecting to one of the repositories then this may adversely affect authentication to all other PassPort repositories. The solution is to either fix the connection issues or remove the failing repository definition.

Operating system support

- This release is built on JRE 8, which is not supported in Solaris 32-bit. Therefore, this version of API Gateway is not supported on Solaris.

OAuth provider upgrade

If you have configured a custom OAuth 2.0 provider, you must ensure that the appropriate class for your provider is set before upgrading to API Gateway version 7.4.1. For example, you might have configured an OAuth provider for a third-party API from Salesforce, Google, or Microsoft.

Perform the following steps before upgrading to version 7.4.1:

1. In your API Gateway 7.4.0 installation, enter the following to start the Entity Store (ES) Explorer tool:

   ```
   INSTALL_DIR/apigateway/posix/bin/esexplorer
   ```

2. Connect to your version 7.4.0 configuration store, for example:

   ```
   INSTALL_DIR/groups/group-2/conf/27aafb6b-6be5-4499-893f-
   178111e23b99/configs.xml
   ```

3. Under **System Components > Auth Profiles > OAuth2**, select your OAuth provider profile (for example, **SalesForce**).
4. Set the **class** field for your `OAuthProviderProfile` type as appropriate (for example, `com.vordel.oauth.client.providers.OAuth2ProviderSalesForce`). If this field does not already exist, right-click under **Field** on the right, and select **Create a class**.
5. Click **Update** to apply your changes.
6. Restart the API Gateway instance.
7. Upgrade to version 7.4.1.

For more details on upgrading, see the *API Gateway Installation Guide*.

Documentation

This section describes documentation enhancements and related documentation.

Documentation enhancements

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

Related documentation

Axway API Gateway is accompanied by a complete set of documentation, covering all aspects of using the product. Go to Axway Sphere at https://support.axway.com to find all documentation for this product version.

For more information about API Gateway and how it is used in Axway 5 Suite, refer to:

- *Axway 5 Suite Overview*
- *Axway 5 Suite Supported Platforms*

Support services

The Axway Global Support team provides worldwide 24 x 7 support for customers with active support agreements.
Email support@axway.com or visit Axway Sphere at https://support.axway.com.

Copyright © 2015 Axway. All rights reserved