Axway API Gateway 7.5.1 Release Notes

Document version: 21 December 2016

Summary

API Gateway is available as a software installation, a physical or virtual appliance, or as a managed service on Axway Cloud.

The software installation is available on Windows and Linux. For more details on supported platforms for software installation, see the *API Gateway Installation Guide*.

The physical appliance is a pre-hardened appliance running the API Gateway runtime delivered on a Dell PowerEdge server. The virtual appliance is a prehardened appliance running the API Gateway runtime and is available as VMware and as an Amazon Machine Image (AMI).

For more details on appliance options, see the *API Gateway Appliance Installation and Administration Guide*.

For best performance, after installing API Gateway 7.5.1, it is recommended to install API Gateway 7.5.1 Service Pack 1.

New features and enhancements

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

Axway Documentation portal

You can find the latest information and up-to-date user guides on the Axway Documentation portal.

Database support

This version adds support for the following database versions:

- Microsoft SQL Server 2014
- MySQL 5.7

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

Easier upgrades

- The API Gateway upgrade flow has been improved:
  - `export`, `upgrade`, and `apply` are now separate steps.
  - Each part of the flow provides instructions for the next step.
  - Stopping at the `upgrade` step allows you to test your existing configuration with the upgrade, and resolve any issues that might arise.
  - The `status` command shows you which node you are upgrading and where you are in the process.
  - Downtime is only required before the `apply` step.
  - The `clean` command lets you revert the system back to its original state.
- The visual upgrade of your API Gateway in Policy Studio helps you detect and analyze upgrade issues in detail:
  - Identify issues or potential behavior changes between versions.
  - Quickly spot the critical issues that you need your attention first.
  - Keep track of your progress and mark issues completed after resolving them.
- *API Gateway Upgrade Guide*:
  - The API Gateway upgrade is covered in its own guide and in more detail.
  - The instructions have been made clearer, in particular for upgrading multi-node configuration.
- Improved logging:
  - The log messages for issues and resolution have been improved.
  - Pre-validation of the environment is included in the log file.
- Improved security:
  - Certificates are regenerated to ensure that old and new processes cannot communicate with each other.
- Installation
  - The instructions on the installer screens have been made clearer.

For more details, see the *API Gateway Upgrade Guide*.

Team Development in Policy Studio

- New project-based architecture – you can create a development project in the file system instead of connecting to a running server:
  - Multiple developers can work in parallel on the same configuration.
  - Use a source code management (SCM) system for continuous integration (CI) and continuous delivery (CD).
  - Separate each API as a project of its own in Policy Studio.
  - Link the individual API projects with a common project that shares global entities between the API projects, avoiding duplication.
  - API projects can call out through **Policy Shortcut** filters to reuse, for example, security filters from Authentication or Authorization categories defined in the common project.
  - Existing customers can still connect directly to a server and create a project from a running Gateway instance.
- The Policy Studio navigation has been updated to be more intuitive and to better support Team Development.

For more details, see the *API Gateway DevOps Deployment Guide* and the *API Gateway Policy Developer Guide*.

Build & Deploy tools

- The build and deployment scripts automate the manual effort in deploying a configuration to API Gateway:
  - Implement production-ready CI for API Gateway applications.
  - The build script `projpack` combines multiple Policy Studio projects to a deployable archive (`.fed` or `.pol`).
  - The deployment script `projdeploy` promotes and deploys an archive to a selected environment, such as a test or production environment.

For more details, see the *API Gateway DevOps Deployment Guide*.

Continuous Integration & Deployment

- When a developer makes changes to a project and pushes changes to the SCM, a CI script, like Jenkins, then:
  - Pulls all projects from the SCM (like Git),
  - Runs `projpack` script to merge the projects into a single configuration,
  - Stores the configuration in a repository, such as Artifactory,

- Uses a tool to provision a test environment, like Chef recipe,
  - The installer `C:\Axway-7.5.1\apigateway\samples\chef` includes a sample Chef cookbook containing recipes to install, configure, start, perfom a health check, deploy, stop and uninstall the API Gateway and Admin Node Manager.
- Runs `projdeploy` script to deploy the configuration to the test environment, and
- Runs customer-specific and API or policy-specific automation tests to check that the APIs and policies are all still working.

For more details, see the *API Gateway DevOps Deployment Guide*.

External Apache Cassandra architecture

- The API Gateway topology has been separated from the Cassandra cluster, and Cassandra is now an independent, installable component running outside the API Gateway process:
  - Install Cassandra with API Gateway, or use your existing Cassandra database.
  - Host multiple groups on the same Cassandra cluster isolated from each other.
  - Run Cassandra and API Gateway on separate machines.
  - Set up Cassadra High Availability (HA) easily.
- User authentication from API Gateway to Cassandra over TLS improves security.
- Cassandra has been upgraded to the latest stable version, v2.2.5, which offers much better support for Windows.

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

Improved WebSocket protocol implementation

- The implementation of WebSocket fragment parsing, encoding, and decoding has been re-factored to be Autobahn-compliant (http://autobahn.ws/).
- Autobahn Testsuite provides a fully automated test suite to verify the specification conformance and implementation robustness of the client and server WebSocket protocol implementations.
- The WebSocket processing pipeline architecture has also been improved. During testing, 10,000 transactions per second over 500 connections on a single API Gateway (on virtual machines with 4 CPUs/2 Cores, 4 GB RAM) were achieved, when using 3 KB messages with simple inbound and outbound policies over SSL connections.

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

Visual Mapper (Restricted Availability)

Policy Studio includes data maps and the Visual Mapper tool for transformations and creating XSLT-based mappings using the format descriptions of the messages, XML schema and JSON schema. Visual Mapper is easy to learn and use, and offers you real-time validation for the operations performed and local simulation of the map. You can use the developed maps to create policies in Policy Studio .

- Design XSLT-based mappings in a graphical way with the Data Map Editor:
  - The editor displays the source and target tree structures.
  - The editor reloads the map if the schemas are changed.
  - You can search for the elements, and view the type or cardinality for each element.
- Link elements together quickly:
  - Drag and drop source elements onto target elements to create links.
  - Replace and reconnect the links as needed.
  - The links provide information how each element in the target schema can be created from the elements in the source schema.
- Modify the values of source elements using predefined XSLT string and formatting functions.
- Add conditionality to element and structure mappings with `if` instructions.
- Store temporary values in variables, and use parameters to receive external values in runtime.
- Design maps faster with automatic linking.
- Simulate the map locally without deploying the configuration to API Gateway.

For more details on data maps, see the *API Gateway Policy Developer Guide*. For more details on Visual Mapper, see the *API Gateway Visual Mapper User Guide*.

Deprecated features

The following features have been deprecated in this release:

- File-based Key Property Store (KPS) has been deprecated, and will be removed in a future release. For details on configuring KPS data stores, see the *API Gateway Key Property Store User Guide*.
- Support for Oracle Access Manager 10g in Policy Studio has been deprecated, and will be removed in a future release. Use the Oracle Access Manager 11g instead. For more details, see the *API Gateway Policy Developer Guide*.

Removed features

Operating system support

This version no longer supports the following platforms:

- Red Hat Enterprise Linux 5
- Oracle Linux 5
- Centos 5
- Solaris 10
- Windows Server 2008 R2
- Windows Server 2008

Database support

This version no longer supports the following databases:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- IBM DB2 9.7
- MySQL 5.1

Browser support

This version no longer supports the following browsers:

- Internet Explorer 8, 9, and 10

API Gateway features

The following features have been removed in this release:

- The **Contivo transformation** filter in Policy Studio has been removed. For transformations, Visual Mapper is now recommended instead . For details on configuring data maps, see the *API Gateway Policy Developer Guide*. For details on using the Visual Mapper tool, see the *API Gateway Visual Mapper User Guide*.
- Direct Internet Message Encapsulation (DIME) messages are no longer supported by API Gateway. Use Multipurpose Internet Mail Extensions (MIME) instead.

- The API Gateway product documentation is no longer available in the `INSTALL_DIR/apigateway/docs` directory. The latest version is now available online at docs.axway.com instead.

Fixed issues

The fixes for issues included in API Gateway v7.4.1 SP1 and SP2 are also included in API Gateway v7.5.1.

Internal ID	Case ID	Description
RDAPI-100	773165	**Issue**: Issues with traffic monitoring files handling. **Resolution**: Previously, the **Maximum number of transaction files** filter was not honored, if you set the value less than 6. Now, the filter is honored also with values less than 6. The information on the minimum target transaction file size (1 MB) was added to Policy Studio.
RDAPI-101	00823373	**Issue**: Failure path for the **Set Attribute** filter not failing. **Resolution**: Previously, you could configure a failure path for the **Set Attribute** filter even though there were no cases where it would ever fail. Now, you cannot configure a failure path for the **Set Attribute** filter. This does not affect filters that are already configured to work with a failure path.
RDAPI-102	00823373	**Issue**: Failure path for the **Remove Attribute** filter not failing. **Resolution**: Previously, you could configure a failure path for the **Remove Attribute** filter even though there were no cases where it would ever fail. Now, you cannot configure a failure path for the **Remove Attribute** filter. This does not affect filters that are already configured to work with a failure path.
RDAPI-126	782828	**Issue**: All users in API Gateway Analytics reflected as `admin`. **Resolution**: Previously, after logging in to API Gateway Analytics, any user was always displayed as `admin`. When logging back in, you were never prompted for a user name and password. Now, your user information is displayed correctly after logging in. When you log back in, you are now prompted for a user name and password.

Internal ID	Case ID	Description
RDAPI-132	790440	**Issue**: Error on invalid credentials after editing the API Gateway host address in Policy Studio. **Resolution**: Previously, editing the API Gateway host address in Policy Studio might corrupt the connection URL. Now, editing the host address does not corrupt the connection URL.
RDAPI-142	782649	**Issue**: `EntityStoreException: Unknown Entity` error when importing a policy extract. **Resolution**: Previously, if you imported a configuration fragment into Policy Studio, you got an error `EntityStoreException: Unknown Entity`. Now, you can import the fragment without errors, and the policies work as expected.
RDAPI-148	771948	**Issue**: `managedomain edit_host` and `add_service_only` create an invalid `init` script. **Resolution**: Previously, the `edit_host` and `add_service_only` options in the `managedomain` script incorrectly set a UID instead of a user name for the service user in the `init` script. Now, `managedomain` sets a user name for the service user in the `init` script.
RDAPI-149	772811	**Issue**: API Gateway reports an error during startup after setting the protocol to use IPv4 only. **Resolution**: Previously, when using IPv4 only, API Gateway attempted to bind to the service port twice, and the second attempt failed with a bind error. Now, when you configure API Gateway to use IPv4 only, it only binds once.

Internal ID	Case ID	Description
RDAPI-202	00800072	**Issue**: Options for a API Gateway group not displayed properly for certain roles. **Resolution**: Previously, the Group menu options were not correctly displayed for certain roles in API Gateway Manager. If an admin user with the roles `API Gateway Operator`, `Deployer`, and `Policy Developer` logged in to API Gateway Manager, and right-clicked a group to view the Group menu options, the only option available in the Group menu was **Lock Group**. After locking the group, it was possible to select **Deploy Configuration**. However, after unlocking the group, all menu options were shown to be available, but only **Deploy Configuration** worked. If the user selected a menu option the user did not have rights to access, the system correctly detected this and logged the user out. Now, when the said admin user logs in, the correct menu options **Lock Group** and **Deploy Configuration** are available in the Group menu. If the group is locked and then unlocked, only these two options are shown as available.
RDAPI-668	00813146	**Issue**: Cannot install Admin Node Manager with script. **Resolution**: Previously, the instructions in *API Gateway Installation Guide* on how to install only API Gateway Node Manager were incorrect. Now, *API Gateway Installation Guide* is updated with correct instructions.
RDAPI-886	782400	**Issue**: The **XML Signature Verification** filter fails when a request uses a SAML assertion with the `Sender Vouches` confirmation method. **Resolution**: Previously, you could not generate or verify XML signatures using the STR-Transform for a SAML 2.0 assertion, because this was not supported. Only SAML 1.0 and 1.1 were supported. Now, generating and verifying XML signatures using the STR-Transform is supported for SAML 1.0, 1.1, and 2.0 assertions.

Internal ID	Case ID	Description
RDAPI-993	00808767	**Issue**: POP3 listener stops without any reason. **Resolution**: Previously, a POP3 listener might stop without logging an error to the trace file. Now, additional logging and an exception handler have been added, so that all errors during POP3 message processing are logged appropriately.
RDAPI-1827	—	**Issue**: Policy Studio's proxy password field is a normal text input box instead of a password input box. **Resolution**: Previously, the proxy password field in Policy Studio was displayed as a normal text input box, causing a security risk. Now, the proxy password field in Policy Studio is displayed securely.
RDAPI-1852	784566	**Issue**: File transfer service requires the path in the style of the Policy Studio host. **Resolution**: Previously, the directory path validation in the file transfer service configuration dialogue in Policy Studio was host dependent. For example, you could not specify a Linux file path on a Windows host. Now, path validation is independent of the host. You can now specify a Linux file path on a Windows host, or a Windows file path on a Linux host.
RDAPI-1867	—	**Issue**: Misspelling in the *API Gateway Policy Developer Guide* v7.4.1. **Resolution**: Previously, the Web Service filter chapter in the *API Gateway Policy Developer Guide* contained a small misspelling in the Monitoring Options section. Now, the misspelling has been fixed.
RDAPI-2333	00811161	**Issue**: Prevent ClickJacking in API Gateway Manager. **Resolution**: Previously, API Gateway Manager UI was not protected against ClickJacking. Now, the Node Manager web server returns new HTTP headers (`Content-Security-Policy` and `X-Frame-Options`) to protect browsers against ClickJacking.

Internal ID	Case ID	Description
RDAPI-2334	00820769	**Issue**: Policy import does not recognize a change to the filter parameter list. **Resolution**: Previously, if you tried to import changes to **Validate REST Filter**, The changes were not correctly detected, and you got the report `The imported configuration contains no applicable differences`. Now, your imported changes to the **Validate REST Filter** are correctly detected on import.
RDAPI-2377	00808783	**Issue**: Traffic Monitor trace level not in sync with system-level trace level. **Resolution**: Previously, Traffic Monitor displayed data level records in the trace output panel regardless of what trace level you had set on the corresponding interface. Now, Traffic Monitor displays data in the trace output panel and the request/response panel like you define in the corresponding interface.
RDAPI-2453	—	**Issue**: Performance issues with the **XML to JSON** and **JSON to XML** filters. **Resolution**: Previously, the **XML to JSON** and **JSON to XML** filters did not perform as well as possible, because factory objects were created per request. Now, avoiding the recreation of the factory object for each request has doubled the performance of these filters.
RDAPI-2608	00824002	**Issue**: The **Retrieve from or write to database** filter fails with `NullPointerException` when the **Date** column contains `null`. **Resolution**: Previously, if you ran a query on **Retrieve from or write to database** filter that retrieved the **Date** column, the filter failed with a `NullPointerException` if the column in the database contained the field value `null`. Now, if you run a query that retrieves the **Date** column containing the value `null`, the **Retrieve from or write to database** filter proceeds. If you have set the system property `ALLOW_NULL_VALUES_FROM_DB` to `false` (the default value), the field is not added to the list of attributes the filter generates. If you have set the property to `true`, the filter adds the field to the list of attributes with the value of `""`.

Internal ID	Case ID	Description
RDAPI-2650	00811161	**Issue**: Prevent ClickJacking in API Gateway Analytics UI. **Resolution**: Previously, the API Gateway Analytics UI was not protected against ClickJacking. Now, the web server returns new HTTP headers (`Content-Security-Policy` and `X-Frame-Options`) to protect browsers against ClickJacking. In addition, the main HTML page includes JavaScript code to detect iframes.
RDAPI-2713	—	**Issue**: KPS is failing for `Map<String, Boolean>`. **Resolution**: Previously, you could not update a property of the type `Map<String, Boolean>` in the KPS browser in API Gateway Manager. Now, you can update a `Map<String, Boolean>` property in the KPS browser in API Gateway Manager.
RDAPI-2728	00807346	**Issue**: How to hide internal server endpoints in an exposed WSDL. **Resolution**: Previously, API Gateway exposed external locations in WSDL and XSD import instructions. Now, API Gateway replaces external locations with locations identified by their fingerprint that API Gateway can render.
RDAPI-2811	00816118	**Issue**: API Gateway becomes unresponsive after a deployment failure. **Resolution**: Previously, API Gateway might become unresponsive on deployment failure, because it was waiting for the running services to complete. Now, in case of a deployment failure, API Gateway can use a deployment timeout and respond, if the running services cannot complete in time.
RDAPI-2813	—	**Issue**: Schema validation is failing in API Gateway v7.4.1 when comparing to v7.2.2. **Resolution**: Previously, `schema-full-checking` was disabled in XSD validation to provide stronger validation, but no toggle was made to disable `schema-full-checking`. Now, you can disable `schema-full-checking` using a configuration fragment `<VMArg name="-DschemaFullChecking=false"/>`.

Internal ID	Case ID	Description
RDAPI-2916	00828431	**Issue**: `JSON Schema does not contain the recommended $schema root node. Are you sure you wish to continue?` when selecting a JSON schema. **Resolution**: Previously, you could not create a data map in Policy Studio using a JSON schema that did not contain a `$schema` version element. Now, you can create a data map with a schema that does not contain a version element.
RDAPI-3001	00830624	**Issue**: **JSON Remove Node** fails if the value of the node to remove is `null`. **Resolution**: Previously, the **JSON Remove Node** filter failed if the value of the node to be removed was set to `null`. Now, the **JSON Remove Node** filter removes the node containing the value `null`.
RDAPI-3050	00826484	**Issue**: Unhandled exception when there is an error in JSON syntax. **Resolution**: Previously, JSON filters were not handling body exceptions correctly and not circuit aborting. This broke fault handling logic where the nearest fault handler in a chain should be executed. Now, JSON filters correctly handle exceptions and abort, ensuring that the nearest fault handler in the chain is executed.
RDAPI-3096	—	**Issue**: Problem running `sysupgrade` from API Gateway v6.3.1 on Windows. **Resolution**: Previously, if you tried `sysupgrade` from the API Gateway v6.3.1 on Windows, the upgrade failed because a file was missing file. Now, you can successfully upgrade v6.3.1 on Windows with `sysupgrade`.
RDAPI-3117	00829419	**Issue**: `VIDUSR` cookie does not use the `secure` and `httponly` flags. **Resolution**: Previously, if you clicked **Policies > Protect Management Interfaces > Create Session** to configure a new Node Manager, the **Session sent over SSL only** and **HTTP Only cookie** check boxes in the **Create Session** filter were not selected by default. Now, both check boxes are selected by default.

Internal ID	Case ID	Description
RDAPI-3127	—	**Issue**: PGP key not updated after reconnecting Policy Studio to API Gateway. **Resolution**: Previously, PGP key configuration was not updated in Policy Studio after you reconnected Policy Studio to an API Gateway instance. Now, PGP key configuration is updated correctly in Policy Studio.
RDAPI-3211	00831687	**Issue**: **PGP Encrypt and Sign** symmetric key algorithm does not take into account if **Encrypt and Sign in Two Passes** is selected. **Resolution**: Previously, the **PGP Encrypt and Sign** filter was using CAST5 instead of the user-defined symmetric-key algorithm for processing. Now, the **PGP Encrypt and Sign** filter always uses the user-defined symmetric-key algorithm.
RDAPI-3230	00829293	**Issue**: Connection filters are no longer working after applying OpenSSL 1.0.1s-fips. **Resolution**: Previously, API Gateway with OpenSSL 1.0.1s-fips was disregarding settings to enable SSLv2 protocol. Now, API Gateway respects configuration of SSLv2 protocol with OpenSSL 1.0.1s-fips.
RDAPI-3284	—	**Issue**: Cannot set the Java security property in `jvm.xml`. **Resolution**: Previously, you could not configure the Java security property in the `jvm.xml` file in API Gateway, but only in the `java.security` file in Java Runtime Environment (JRE). Now, you can configure the Java security property in the `jvm.xml` file using the `SecurityProperty` node in `JVMSettings`, for example: `<SecurityProperty name="jdk.tls.disabledAlgorithms" value="SSLv3"/>`

Internal ID	Case ID	Description
RDAPI-3292	—	**Issue**: No audit event for changing the login advisory banner. **Resolution**: Previously, the Advisory Banner configuration changes were not logged. Now, the Advisory Banner configuration changes are logged with a dedicated event.
RDAPI-3296	—	**Issue**: API Gateway crashes during an SSL handshake in FIPS mode. **Resolution**: Previously, API Gateway crashed in FIPS mode during an SSL handshake, if the TLS server used `SHA512withECDSA` signature algorithm and the server public key contained a `id-ecPublicKey` key. Now, API Gateway successfully completes the said SSL handshake in FIPS mode.
RDAPI-3340	00835154	**Issue**: Security vulnerabilities identified in OpenSSL Security Advisory [3rd May 2016]. **Resolution**: Previously, API Gateway included OpenSSL 1.0.1p-fips that included security vulnerabilities, such as: • Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800) • Padding oracle in AES-NI CBC MAC check (CVE-2016-2107) Now, API Gateway includes OpenSSL 1.0.1t-fips that addresses known security vulnerabilities. For more details, see OpenSSL Security Advisory [3rd May 2016].
RDAPI-3375	00835645	**Issue**: Unable to migrate Client Application Registry data from API Gateway v7.1.1. **Resolution**: Previously, migrating Client Application Registry data from API Gateway v7.1.1 failed, because the upgrade script `migrateFrom71.py` did not run due to syntax errors. Now, the API Gateway upgrade script `migrateFrom71.py` runs successfully.

Internal ID	Case ID	Description
RDAPI-3452	00832678	**Issue**: **Retrieve from or write to database** failed when trying to insert a `null` value. **Resolution**: Previously, the **Retrieve from or write to database** filter failed with a `NullPointerException` if you ran an `INSERT` statement with the value `null` set for one of the columns. Now, you can run `INSERT` statements with `null` set for columns, if your database schema allows it.
RDAPI-3461	00830013	**Issue**: Cannot handshake anymore with `SSL_RSA_WITH_3DES_EDE_CBC_SHA`. **Resolution**: Previously, the API Gateway FTPS server did not accept an SSL client connection with the `SSL_RSA_WITH_3DES_EDE_CBC_SHA` cipher. Now, the FTPS server accepts an SSL client connection with RSA ciphers.
RDAPI-3462	00820033	**Issue**: API Gateway Analytics `configureserver` does not accept blank `SMTP user/pass`. **Resolution**: Previously, you could not have an empty value for the parameter `smtpuser` in the `configureserver` script in API Gateway Analytics. Now, the script accepts an empty value for `smtpuser`.

Known issues

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

API Manager KPS table definitions is not upgraded correctly

After an upgrade from an earlier API Gateway version with an existing API Manager installation, publishing a new API or an existing unpublished API fails, because the indexing of the KPS table definitions is different.

To avoid this issue, after installing API Gateway 7.5.1 and *before* you upgrade, you must download and install API Gateway 7.5.1 Service Pack 1.

For more details, see *API Gateway Upgrade Guide*.

Export error holding on to KPS resources when upgrading API Gateway (Windows only)

The `sysupgrade export` command calls the old API Gateway version 7.x server to export Key Property Store (KPS) data to JSON files. On Windows, these JSON files are created successfully, but the locks on the JSON files are kept open because the old API Gateway server does not release the locks. For example, this means that if you try to delete the JSON file in Windows Explorer, you get a message that the file cannot be deleted because it is being used by another process. If you try to run `sysupgrade export` again, the export will fail.

The workaround is to restart the old API Gateway instance after each `sysupgrade export`, which releases the locks. To avoid downtime, you should restart each API Gateway instance after each `export` one-by-one.

Issues with the sysupgrade if FIPS is enabled (Windows only)

After upgrading API Gateway on Windows, running `sysupgrade.bat clean` threw an error. This issue has been fixed, but there is another known issue related to this.

During the `apply` step of an upgrade, you are prompted to start Node Manager on the new version 7.5.1 installation. If FIPS is enabled, Node Manager fails to move two files to the `jce-inactive` folder. This only happens on a Windows system and only if FIPS enabled.

The workaround is to start Node Manager when prompted, let the `apply` step complete, and then stop and restart Node Manager.

API Manager users cannot complete registration after upgrading API Gateway

New users that were registered in API Manager before an upgrade, but who did not complete registration by activating their account with the link provided in email, cannot complete registration after upgrade.

These users must be re-registered in API Manager after the upgrade is complete.

Apache Cassandra required for upgrade when not used in earlier API Gateway version

When upgrading to API Gateway v7.5.1 from an earlier version, you must install Apache Cassandra even when it was not used in the earlier version.

For details on installing Cassandra, see the *API Gateway Installation Guide*. For details on upgrading from an earlier version, see the *API Gateway Upgrade Guide*.

Cassandra JRE bundled with API Gateway

When installing Cassandra, you are prompted to specify a JRE for Cassandra. You can select the default JRE bundled with API Gateway. However, this default JRE has the following limitations on Windows:

- Running Cassandra with this 32-bit JRE limits the maximum amount of memory available to Cassandra on 64-bit systems
- You cannot use this JRE to run Cassandra as a Windows Service

It is recommended to download and install a separate JRE before installing Cassandra on Windows, and select this JRE during Cassandra installation. Cassandra requires the latest version of JRE 8.

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

Problem with Cassandra authentication (Windows only)

If you have configured Cassandra authentication, the authentication fails with an incorrect user name or password exception. However, the `cqlsh` connection to Cassandra using the same user name and password is successful.

The workaround is to change the value for `authorizer` and `authenticator` to `AllowAllAuthenticator` in the following file:

```
CASSANDRA_HOME\conf\cassandra.yaml
```

Powershell script execution policy

Modern Windows versions support the new PowerShell command-line interpreter. The Cassandra installation provides both the old `.bat` and the new `.ps1` startup files.

When you run the `cassandra` command in `CASSANDRA_HOME\bin`, it runs either in the legacy startup mode or the new startup mode depending on the PowerShell script execution policy setting. If this policy is set to `Unrestricted`, the new PowerShell startup script runs. Else, the legacy startup script runs.

The startup behavior and command line options are different depending on the type of startup. For more details, see the *API Gateway Installation Guide*.

TLS for non-default JRE

If you select an alternative JRE instead of the default JRE during the installation and want to enable Cassandra to use TLS, you must install Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction policies for your JRE.

Cassandra on API Gateway Appliance

The `cqlsh` command is not supported on API Gateway Appliance. For more details, see the *API Gateway Installation Guide*.

Code samples

The code samples `\DEVELOPER_GUIDE\jabber` and `DEVELOPER_GUIDE\restJabber` are missing from the `<INSTALL_DIR>/apigateway/samples/developer_guide` directory. You can download these code samples from Axway Sphere at https://support.axway.com.

WebSocket protocol

- If you use `%h` in the Access Log initial string, the HTTP Long Polling connections have a time delay at the API Gateway. WebSocket connections are not affected.
- Adding the same URL for a WebSocket path and a HTTP path is not supported. You get an error message, if you try this in Policy Studio.

JWT Filters

When you operate in FIPS mode, the implementation from the default, non-FIPS provider is invoked, if any of the following algorithms is selected in the JWT Signing filter:

- RSASSA-PSS using SHA-256 and MGF1 with SHA-256
- RSASSA-PSS using SHA-384 and MGF1 with SHA-384
- RSASSA-PSS using SHA-512 and MGF1 with SHA-512

To avoid this, disable the Bouncy Castle Crypto Provider in the `/system/conf/jvm.xml` file. When the JWT Signing filter with one of the above algorithms selected is called, the filter fails with the following error:

```
ERROR 18/Apr/2016:16:24:39.275 [4a48:17e014570200451f205ec316] java exception:
com.vordel.circuit.jwt.JWTException: com.nimbusds.jose.JOSEException:
Unsupported RSASSA algorithm: SHA512withRSAandMGF1 Signature not available
```

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

Documentation

This section describes documentation enhancements and related documentation.

Axway Documentation portal

You can find the latest information and up-to-date user guides on Axway Documentation portal.

Documentation enhancements

The following new user guides have been added in this release:

- *API Gateway Upgrade Guide*
- *API Gateway DevOps Deployment Guide*

The following user guides have been updated in this release:

- *API Gateway Installation Guide*
- *API Gateway Concepts Guide*
- *API Gateway Administrator Guide*
- *API Gateway Policy Developer Guide*
- *API Gateway Developer Guide*
- *API Gateway OAuth User Guide*
- *API Gateway Appliance Installation and Administration Guide*
- *API Gateway Security Guide*
- *API Gateway Key Property Store User 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.