OpenIG Release Notes

Version 3.1.0

Mark Craig

ForgeRock AS
33 New Montgomery St.,
Suite 1500
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Notes covering OpenIG prerequisites, fixes, known issues. OpenIG provides a high-performance reverse proxy server with specialized session management and credential replay functionality.

Table of Contents

Chapter 1

What's New in OpenIG

OpenIG 3.1.0 fixes a number of issues, and provides the following additional features.

- OpenIG can now store session information in encrypted JSON Web Token (JWT) cookies on the user-agent (OPENIG-224, OPENIG-278). By default, OpenIG continues to back session information with HttpSession from the container where OpenIG runs.

  With this change, you can specify the session storage at the global level, or in a particular route configuration. For details, see JwtSession and *Setting Up Keys For JWT Encryption*.

- OpenIG now allows you to inline configuration objects (OPENIG-311), to omit "config" fields when all values are optional (OPENIG-300), to omit the "objects" field from the "heap" OPENIG-380), and even to omit the "heap" when it is empty or would only contain a single handler (OPENIG-329).

  When you bring an object inline, you no longer need to specify the "name".

  For example, suppose your former `config.json` file looks like this:

```
{
    "heap": {
        "objects": [
            {
                "name": "Chain",
                "type": "Chain",
                "config": {
                    "filters": [
```

```
                        "ReplaceHostFilter"
                    ],
                    "handler": "Router"
                }
            },
            {
                "name": "ReplaceHostFilter",
                "type": "HeaderFilter",
                "config": {
                    "messageType": "REQUEST",
                    "remove": [
                        "host"
                    ],
                    "add": {
                        "host": [
                            "example.com"
                        ]
                    }
                }
            },
            {
                "name": "Router",
                "type": "Router",
                "config": {}
            }
        ]
    },
    "handler": "Chain"
}
```

OpenIG now lets you rewrite the `config.json` file like this:

```
{
    "handler": {
        "type": "Chain",
        "config": {
            "filters": [
                {
                    "type": "HeaderFilter",
                    "config": {
                        "messageType": "REQUEST",
                        "remove": [
                            "host"
                        ],
                        "add": {
                            "host": [
                                "example.com"
                            ]
                        }
                    }
                }
            ],
            "handler": {
                "type": "Router"
            }
        }
    }
}
```

Examples in the documentation now use streamlined configurations where it makes sense.

- OpenIG now supports object decorators (OPENIG-340). Decorators allow you to define heap objects that decorate other objects, adding the new behavior that the decorator provides.

  OpenIG provides the following decorators out of the box.

  - A CaptureDecorator that extends what the CaptureFilter could do to capture requests, responses, and exchange data on any decorated object (OPENIG-299, OPENIG-301)
  - A TimerDecorator that records times to process the exchange through any decorated object (OPENIG-352, OPENIG-353)
  - An AuditDecorator that allows you to audit operation for any decorated object.

  For detailed information about decorators, see the *Reference* on *Decorators*.

- OpenIG now provides a publish-and-subscribe audit framework and a sample monitoring handler that returns basic statistics (OPENIG-359, OPENIG-386). To learn more, start by reading the chapter about the *OpenIG Audit Framework*.
- OpenIG script configurations can now include arguments (OPENIG-240).
- The OAuth2ClientFilter and OAuth2ResourceServerFilter now cache data to avoid unnecessarily calls to the provider (OPENIG-350).
- OpenIG uses improved object names in log messages that make it easier to identify the source of the message (OPENIG-358, OPENIG-371).
- The OpenIG Exchange now provides information about the client (OPENIG-333).

  For details see the *Reference* on *ClientInfo*.

Chapter 2

Before You Install

This chapter covers requirements for running OpenIG software.

Tip

If you have a special request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com.

2.1 JDK Version

This release of OpenIG requires Java Development Kit 6, 7, or 8. ForgeRock recommends the most recent update to ensure you have the latest security fixes.

If you install an OpenAM policy agent in the same container as OpenIG, then you must use a Java release that is supported with the policy agent as well.

2.2 Web Application Containers

OpenIG runs in the following web application containers.

- Apache Tomcat 7
- Jetty 8 (8.1.13 or later)

You must deploy OpenIG to the root context of the container. Deployment in other context causes unexpected results, and cannot be supported.

OpenIG expressions depend on Unified Expression Language 2.2, which is available in containers that support Servlet 3.0 or later. Some expressions can lead to a `java.lang.NoSuchMethodError` in containers that support only Servlet 2.5 (and EL 2.1).

See the *Guide to OpenIG* section, *Configuring Deployment Containers*, for details on setting up your web application container.

Chapter 3

Changes & Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

3.1 Important Changes to Existing Functionality

This release includes configuration changes compared to OpenIG 3.0.0. See Section 3.2, “Deprecated Functionality” for a list of configuration changes resulting in deprecation of earlier features.

3.2 Deprecated Functionality

This release deprecates the following configuration settings. Deprecation is defined in the *Reference* appendix on *ForgeRock Product Interface Stability*.

Table 3.1. Configuration settings

Configuration Object	Deprecated Settings	Newer Evolving Settings
CaptureFilter	Entire object	Use a CaptureDecorator instead
gateway servlet	"handlerObject"	New name: "handler"
	Deprecated format: `"heap": { "objects":`	New format: `"heap": [ configuration object, ... ]`

Configuration Object	Deprecated Settings `[ configuration object, ... ] }`	Newer Evolving Settings
HttpClient	"keystore"	Replaced by "keyManager", which takes one or more KeyManager names
	"truststore"	Replaced by "trustManager", which takes one or more TrustManager names
OAuth2ResourceServerFilter	"enforceHttps"	New name: "requireHttps"
	"httpHandler"	New name: "providerHandler"
	"requiredScopes"	New name: "scopes"
RedirectFilter	Entire object	Use LocationHeaderFilter instead
Route	Deprecated format: `"heap": { "objects": [ configuration object, ... ] }`	New format: `"heap": [ configuration object, ... ]`

This release deprecates the following API classes, which are likely to be removed in a future release.

- org.forgerock.openig.filter.CaptureFilter
- org.forgerock.openig.heap.NestedHeaplet

3.3 Removed Functionality

No functionality has been removed in this release.

Chapter 4

Fixes, Limitations, & Known Issues

OpenIG issues are tracked at https://bugster.forgerock.org/jira/browse/OPENIG. This chapter covers the status of key issues and limitations at release 3.1.0.

4.1 Fixes

The following issues were fixed in release 3.1.0.

- OPENIG-370: Log output often includes irrelevant or duplicated information
- OPENIG-368: OAuth2ClientFilter rebases client endpoint against possibly rebased request.uri
- OPENIG-331: Moving a file in Routes may result in no route configured
- OPENIG-325: Allow scripts and AssignmentFilters to update exchange.request.uri
- OPENIG-312: Use Jackson for better messages about configuration errors in JSON
- OPENIG-119: RedirectFilter should handle HTTP 301
- OPENIG-85: SqlAttributesFilter throws SQLException: Invalid operation for forward only resultset
- OPENIG-78: SqlAttributesFilter throws SQLException: Invalid column index
- OPENIG-56: Temporary files leak

- OPENIG-30: OpenIG to protect multiple apps at one location

The ForgeRock issue tracker gives you access to the complete list of resolved issues.

4.2 Limitations

For HTTPS, OpenIG can check server certificates. However mutual authentication, where OpenIG presents its client certificate, is not supported if the client certificate is not the first certificate in the HttpClient key store.

OpenIG scripts are not sandboxed, but instead have access to anything in their environment. You must make sure that the scripts that OpenIG loads are safe.

When acting as an OpenID Connect 1.0 relying party, OpenIG does not support dynamic registration.

4.3 Known Issues

The following known issues remained open at the time release 3.1.0 became available.

- OPENIG-322: Cannot access both an OpenAM (self-signed) and a Google HTTPS endpoint
- OPENIG-290: Null pointer exception when capturing SAML federation response
- OPENIG-258: OpenIG doesn't shutdown properly when protected by a Tomcat J2EE agent
- OPENIG-234: Federation doesn't work if we used incomplete user in IDP

Chapter 5

How to Report Problems & Provide Feedback

If you have questions regarding OpenIG that are not answered by the documentation, there is a mailing list which can be found at https://lists.forgerock.org/mailman/listinfo/openig where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenIG, report them in https://bugster.forgerock.org.

When requesting help with a problem, include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Machine type, operating system version, web container and version, Java version, and OpenIG release version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant logs or stack traces

Chapter 6

Support

You can purchase OpenIG support, subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see http://forgerock.com/partners/find-a-partner/.