



Release Notes

OpenIG 3.0.0

Mark Craig

ForgeRock AS
33 New Montgomery St., Suite
1500
San Francisco, CA 94105, USA
+1 415-523-0772
www.forgerock.com

Copyright © 2012-2017 ForgeRock AS.

Abstract

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



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

ForgeRock® and ForgeRock Identity Platform™ are trademarks of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong @ free . fr.

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <http://fontawesome.io>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>.

Table of Contents

1. What's New in OpenIG	1
2. Before You Install	3
2.1. JDK Version	3
2.2. Web Application Containers	3
3. Changes & Deprecated Functionality	4
3.1. Major Changes to Existing Functionality	4
3.2. Deprecated Functionality	5
3.3. Removed Functionality	5
4. Fixes, Limitations, & Known Issues	6
4.1. Fixes	6
4.2. Limitations	6
4.3. Known Issues	7
5. How to Report Problems & Provide Feedback	8
6. Support	9

Chapter 1

What's New in OpenIG

OpenIG 3.0.0 fixes a number of issues, and provides the following additional features.

- This release brings major improvements to the configuration model.

OpenIG now supports runtime configuration changes, with separate routes for separate applications (OPENIG-73, OPENIG-97, OPENIG-204). For a tutorial on how to use routes, see *Routing Tutorial* in the *Gateway Guide*.

OpenIG now removes the Java EE Servlet and Servlet Filter objects to simplify configurations. The top-level configuration object now references a handler rather than a Servlet (OPENIG-95).

OpenIG now supports the ability to change the location where configuration files are stored (OPENIG-96, OPENIG-140).

- OpenIG now supports OAuth 2.0 and OpenID Connect 1.0 (OPENIG-176, OPENIG-195).

OpenIG can act as an OAuth 2.0 resource server on behalf of a server housing protected resources. For details and a tutorial demonstrating this capability see the chapter, *Configuring OpenIG as an OAuth 2.0 Resource Server* in the *Gateway Guide*.

OpenIG can act as an OAuth 2.0 client application, and as an OpenID Connect 1.0 relying party. For details and a tutorial demonstrating these capabilities see the chapter, *Configuring OpenIG as an OAuth 2.0 Client* in the *Gateway Guide*.

- OpenIG now supports use of scripts to process and to handle the HTTP exchange (OPENIG-66, OPENIG-72, OPENIG-80, OPENIG-90, OPENIG-92, OPENIG-235). Use the `ScriptableFilter` and `ScriptableHandler` objects to the configuration in order to hook scripts into exchange processing. At present Groovy is supported, but JavaScript is not. For examples using Groovy scripts for Filters and Handlers see the chapter, *Scripting Filters & Handlers* in the *Gateway Guide*.

Scripting also adds support for working with LDAP servers (OPENIG-81).

- OpenIG now includes a default welcome page if no configuration is found (OPENIG-202).
- SAML 2.0 federation support is now integrated into the main OpenIG .war file (OPENIG-94).

OpenIG SAML 2.0 federation now supports SP-initiated single logout and also supports single logout using the SOAP binding (OPENIG-10, OPENIG-237).

OpenIG SAML 2.0 federation now supports an option to set AuthnContext in the OpenIG session (OPENIG-9). You can also obtain OpenAM authentication level by including the `AuthLevel` attribute in the IDP or SP attribute mapping.

- OpenIG Expressions now support additional built-in functions, and use of system properties and environment variables.

Built-in functions to call within expressions now include `base64Encode(string)`, `base64Decode(string)`, `matchingGroups(string, pattern)`, `read(filename)`, `readProperties(filename)`, `urlencode(string)`, and `urlDecode(string)` as described in the reference section, Functions in the *Reference* (OPENIG-54, OPENIG-213).

Expressions access system properties and environment variables as described in the reference section, Expressions in the *Reference*.

Expressions now also support Java Beans (OPENIG-200).

- OpenIG Expressions are now usable in more configuration fields (OPENIG-12, OPENIG-211, OPENIG-232).
- OpenIG now provides an HttpClient configuration object that lets you disable connection reuse when server does not support it, set socket and connection timeouts, choose how you verify host names in server certificates, and so forth (OPENIG-12, OPENIG-38, OPENIG-203).
- OpenIG now allows you to change URI components, rather than rewrite entire URIs (OPENIG-70, OPENIG-243).
- OpenIG now provides a RedirectFilter to rewrite Location headers returned as a result of a HTTP redirect (OPENIG-35).
- OpenIG StaticRequestFilter now lets you restore the original state of the request (OPENIG-245).
- OpenIG HttpBasicAuthFilter now lets users change their passwords during a session (OPENIG-32).

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)

See the *Guide to OpenIG* section, *Configuring Deployment Containers* in the *Gateway Guide*, 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. Major Changes to Existing Functionality

This release brings important new functionality and many changes to OpenIG.

If you are running older versions of OpenIG you must at minimum modify both the location and also the content of your `config.json` file.

You must migrate the configuration by hand.

- The configuration file location and configuration layout have changed.

By default, configuration files are now stored under `$HOME/.openig/config` and `$HOME/.openig/SAML` on UNIX, Linux, and Mac OS X, and under `%appdata%\OpenIG\config` and `%appdata%\OpenIG\SAML` on Windows systems.

For details the *Guide to OpenIG* section, *Installing OpenIG* in the *Gateway Guide*.

As described in that section, the base configuration directory can be changed and can even be set at run time. You must therefore take care to protect access to OpenIG, both by protecting access to the environment at startup time, and also by protecting access to configuration files at run time.

Notice that OpenIG configuration can be split across multiple files.

- Usage for some configuration objects has changed. In particular, the top-level configuration object now references a Handler rather than a Servlet.

When migrating your configuration, review current usage in the *OpenIG Reference*.

- OpenIG supports runtime configuration changes, as described in the *Guide to OpenIG* chapter, *Routing Tutorial* in the *Gateway Guide*.

Notice that you can turn off runtime configuration changes.

- OpenIG configuration Expressions can depend on runtime settings, such as environment variables and system properties.

You must ensure that these settings are properly protected.

- As SAML 2.0 federation support is now integrated into the main OpenIG .war file, the way of configuring dispatch to the Federation component has changed. For an example of how the configuration is handled now, see the *Guide to OpenIG* chapter, Tutorial For OpenIG Federation in the *Gateway Guide*, or read the example configuration file, *Configuration for the Federation Tutorial* in the *Gateway Guide*.

3.2. Deprecated Functionality

No functionality is deprecated in this release.

3.3. Removed Functionality

Custom Servlet and Servlet Filter integration now requires additional development. For an example, see the [org.forgerock.openig.handler.saml](#) package.

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 3.0.0.

4.1. Fixes

The following issues were fixed in release 3.0.0.

- OPENIG-76: Documentation is not clear about what the CryptoHeaderFilter can encrypt/decrypt
- OPENIG-67: Shutdown problem when using Federation Gateway
- OPENIG-62: StaticRequestFilter overrides the Content-Type header
- OPENIG-59: Federation does not correctly handle XML signatures
- OPENIG-51: SSL mutual auth fails because client certificate is not presented to server
- OPENIG-49: Empty Expression string not handled correctly
- OPENIG-36: Problems with Expression examples in the reference documentation
- OPENIG-31: Cached HttpBasic authentication header can cause issues when a user changes password
- OPENIG-29: Federation requires AssertionMapping settings, even though the mapping is optional
- OPENIG-15: Expressions needed in HeaderFilter and need to support backslashes
- OPENIG-8: OpenIG gateway removes Content-Length: 0
- OPENIG-4: Boundary stripped off of multipart/form-data on POST operation
- OPENIG-1: File upload over HTTPS fails

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 3.0.0 became available.

- OPENIG-258: OpenIG doesn't shutdown properly when protected by a Tomcat J2EE agent
- OPENIG-221: Cannot specify which certificate to present to server if server requires mutual authentication in https
- OPENIG-85: SqlAttributesFilter throws SQLException: Invalid operation for forward only resultset
- OPENIG-78: SqlAttributesFilter throws SQLException: Invalid column index
- OPENIG-69: OpenIG seems to remove the URI part of requests when using baseURI
- OPENIG-56: Temporary files leak

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/>.