



Release Notes

/ ForgeRock Identity Gateway 5.5

Latest update: 5.5.2

Mark Craig
Joanne Henry

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Copyright © 2012-2018 ForgeRock AS.

Abstract

Notes on prerequisites, fixes, and known issues for the ForgeRock® Identity Gateway.



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. See <https://opensource.org/licenses/OFL-1.1>.

Table of Contents

Preface	iv
1. What's New	1
1.1. Maintenance Releases	1
1.2. New Features	1
1.3. Product Improvements	3
1.4. Security Advisories	5
2. Before You Install	6
2.1. Downloading IG Software	6
2.2. JDK Version	6
2.3. Web Application Containers	6
2.4. Features Supported With ForgeRock Access Management	7
2.5. ForgeRock Access Management Policy Agents	8
3. Compatibility With Other Releases	9
3.1. Important Changes to Existing Functionality	9
3.2. Deprecated Functionality	10
3.3. Removed Functionality	11
4. Fixes, Limitations, and Known Issues	14
4.1. Key Fixes	14
4.2. Limitations	15
4.3. Known Issues	16
5. Documentation Changes	18
6. Getting Support	19
6.1. Accessing Documentation Online	19
6.2. How to Report Problems or Provide Feedback	19
6.3. Getting Support and Contacting ForgeRock	20

Preface

ForgeRock Identity Platform™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see <https://www.forgerock.com>.

Chapter 1

What's New

1.1. Maintenance Releases

IG 5.5.2

ForgeRock maintenance releases contain a collection of fixes and minor RFEs that have been grouped together and released as part of our commitment to support our customers. For general information on ForgeRock's maintenance and patch releases, see [Maintenance and Patch Availability Policy](#).

- IG 5.5.2 is the latest release targeted for IG 5.5, and 5.5.1 deployments and can be downloaded from the *ForgeRock Backstage* website. To view the list of fixes in this release, see [Key Fixes in IG 5.5.2](#).

The release can be deployed as an initial deployment or updated from an existing 5.5 or 5.5.1 deployment.

1.2. New Features

What's New in IG 5.5.2

- There are no new features in this release.

What's New in IG 5.5.1

- There are no new features in this release.

IG 5.5

IG 5.5 includes the following new features:

IG Studio

IG Studio has been updated to include the following features:

Sophisticated Throttling Policies

Grouping policies that apply a throttling rate to a single group containing all requests, or to independent groups of requests. Groups can be defined with a standard or custom grouping policy.

Mapping policies that allow custom mapping criteria, and multiple mapped rates in mapped throttling policies.

Creation of Different Filter Types

The following filter types and scripts can now be created in IG Studio: generic filters, scripts, scriptable filters, and scriptable rate policies for throttling filters.

Route Import

Routes can now be imported from external .json files into IG Studio. Routes not created in IG Studio can be viewed in the backend configuration.

Route Editing

The IG Studio editor can be used to edit routes that were created in IG Studio, imported from file, or that exist your backend configuration.

Route Viewing

A route's filters can now be viewed in a chain, and reordered in the chain.

You can view a route's status to see if it is **Undeployed**, **Deployed**, **Changes pending**, or **Out of sync**.

Capture

IG Studio can now capture ForgeRock Identity Platform messages as well as messages about requests and responses that are traversing the route.

Search

IG Studio now includes a search feature to search for routes.

OAuth 2.0

OAuth 2.0 has been updated to include the following features:

OAuth 2.0 Token Introspection

IG now supports the token introspection endpoint, `/oauth2/introspect` to resolve OAuth2 access tokens. In previous releases, only the token info endpoint, `/oauth2/tokeninfo`, was supported.

Use the `/oauth2/introspect` endpoint to retrieve metadata about a token that is not available at the `/oauth2/tokeninfo` endpoint, such as the context in which the token was issued.

For information about the token introspection endpoint, see RFC-7662, *OAuth 2.0 Token Introspection*.

Client Authentication Through `private_key_jwt`

Clients can now authenticate to an OAuth 2.0 authorization server or OpenID Provider using the `tokenEndpointAuthMethod` method `private_key_jwt`.

With `private_key_jwt`, you can configure claims to be used for client authentication during access token retrieval.

For information, see `ClientRegistration(5)` in the *Configuration Reference*.

Scripting to Configure OAuth 2.0 Token Resolution

It is now possible to configure access token resolution by using a script. For information about all configuration options, see the `accessTokenResolver` property of `OAuth2ResourceServerFilter(5)` in the *Configuration Reference*.

Support for IG JBoss EAP

IG can now run in JBoss Enterprise Application Platform (JBoss EAP) version 7.

For information, see "JBoss EAP For IG" in the *Gateway Guide*.

Audit Event Handlers

Support has been added for the Splunk Audit Handler. For information, see `SplunkAuditEventHandler(5)` in the *Configuration Reference*.

1.3. Product Improvements

IG 5.5.2

- There are no major improvements to existing functionality other than bug fixes.

IG 5.5.1

- There are no major improvements to existing functionality other than bug fixes.

IG 5.5

IG 5.5 includes the following improvements:

Default cookie name is `IG_SESSIONID`

Most web containers use `JSESSIONID` as the default cookie name. To prevent invalid session IDs when a protected application uses the same cookie name as the IG web container, IG now uses `IG_SESSIONID` as its default cookie name.

Support for UMA 2.0

Support for UMA 2.0 has been added in this release. Features and functionality have been upgraded to support new UMA standards. Support for earlier versions of UMA has been removed.

For information, see "*Supporting UMA Resource Servers*" in the *Gateway Guide* and `UmaService(5)` in the *Configuration Reference*.

Configuration Expressions For Header Name and Form Parameter Name of `StaticRequestFilter`

Configuration expressions can now be used to create the following properties of the `StaticRequestFilter`:

- `name` field of the property `headers`
- `param` field of the property `form`

This feature provides the flexibility to assign different header names and form parameters when using the same route in different environments. For example, the name of a cookie header can be different in a production or development environment.

For information, see `StaticRequestFilter(5)` in the *Configuration Reference*.

`ClientHandler` Can Declare an HTTP Web Proxy

The `ClientHandler` can now declare an outgoing proxy server such as Squid to submit requests to other parts of the network.

For information, see the `proxy` property of `ClientHandler(5)` in the *Configuration Reference*.

Runtime Expressions for `baseURI` of `DispatchHandler`

Runtime expressions can now be used to define the `baseURI` property of `DispatchHandler`.

This feature provides the flexibility to change the `baseURI` according to some request attributes.

For information, see `DispatchHandler(5)` in the *Configuration Reference*.

Increased Flexibility for Authentication in `SingleSignOnFilter`

A new property, `loginEndpoint`, is added to the `SingleSignOnFilter` to increase flexibility for authentication. Authentication can be performed through AM or an alternative application, and can include authentication parameters. For information, see the `loginEndpoint` property of `SingleSignOnFilter(5)` in the *Configuration Reference*.

Configuration Expressions in `prefix` and the Reference Configuration Object

Configuration expressions can now be used in the definition of `prefix` and the reference configuration object.

For information, see `reference` in the *Configuration Reference* and `AdminHttpApplication(5)` in the *Configuration Reference*.

Audit Event Fields Case-Insensitive For Filtering

A list of audit event fields can be specified to be considered as case-insensitive for filtering.

For information, see `AuditService(5)` in the *Configuration Reference*.

Support for "scope" in Dynamic Client Registration

As required by RFC 7591, *OAuth 2.0 Dynamic Client Registration Protocol*, the `metadata` property of `OAuth2ClientFilter` now supports `scope`.

Dynamic client registration with versions of AM earlier than 5.5 must use the `scopes` property.

Dynamic client registration with AM 5.5 can use the `scopes` or `scope` property.

For the option to dynamically register with a wider range of identity providers, you can use both `scope` and `scopes` at the same time.

1.4. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see *Security Advisories* in the *Knowledge Base library*.

Chapter 2

Before You Install

This chapter describes the requirements for running IG.

Tip

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

2.1. Downloading IG Software

Download the following product software from the [ForgeRock BackStage](#) download site:

- IG .war file, [IG-5.5.2.war](#)
- Web application for testing IG configurations, [IG-sample-application-5.5.2.jar](#)

2.2. JDK Version

IG runs with the following JDKs:

- Oracle JDK 8
- OpenJDK 1.8

If you are using IG on Tomcat with SSL enabled, use OpenJDK 1.8.0_121 or later versions to prevent mismatch between client side ciphers and server side ciphers.

For the latest security fixes, ForgeRock recommends that you use the most recent update.

If you install an AM policy agent in the same container as IG, you must use a Java release that is also supported by that policy agent.

2.3. Web Application Containers

IG runs in the following web application containers:

- Apache Tomcat 7, 8, or 8.5.x
- Jetty 8 (8.1.13 or later), or 9
- JBoss EAP 7

Important

Support for Tomcat 7 and Jetty 8 (8.1.13 or later) will be removed in a future release.

Deploy IG to the root context of the container. Deployment in other contexts causes unexpected results, and is not supported.

For information about setting up a web application container see "Configuring Deployment Containers" in the *Gateway Guide*.

2.4. Features Supported With ForgeRock Access Management

This section describes the IG features that are supported with AM:

Features Supported With AM

Feature	Supported in AM Version
AM password capture and replay, as described in " <i>Getting Login Credentials From Access Management</i> " in the <i>Gateway Guide</i>	OpenAM 13.5.x, and AM 5.0 and later versions
AM policy enforcement, as described in " <i>Enforcing Policy Decisions and Supporting Session Upgrade</i> " in the <i>Gateway Guide</i>	OpenAM 13.5.x, and AM 5.0 and later versions
OpenID Connect dynamic registration and discovery, as described in " <i>Using OpenID Connect Discovery and Dynamic Client Registration</i> " in the <i>Gateway Guide</i>	OpenAM 13.5.x, and AM 5.0 and later versions
Token transformation, as described in " <i>Transforming OpenID Connect ID Tokens Into SAML Assertions</i> " in the <i>Gateway Guide</i> .	OpenAM 13.5.x, and AM 5.0 and later versions
User Managed Access 2.x, for IG 5.5 and later versions, as described in " <i>Supporting UMA Resource Servers</i> " in the <i>Gateway Guide</i>	AM 5.5
User Managed Access 1.x, for IG 5.0.x and earlier versions	AM 5.1.x and earlier versions
Single sign-on, as described in SingleSignOnFilter(5) in the <i>Configuration Reference</i> .	AM 5 and later

2.5. ForgeRock Access Management Policy Agents

When installing an AM policy agent in the same container as IG, use AM Java EE Policy Agent 3.5. Earlier versions might not shut down properly with the web application container.

Make sure that the container version is supported both for IG and the AM Java EE Policy Agent that you install alongside IG.

AM Java EE Policy Agent 3.5.1 and earlier versions do not support Tomcat 8.5.x or Jetty 9.

Chapter 3

Compatibility With Other Releases

This chapter describes major changes to existing functionality, deprecated functionality, and removed functionality.

3.1. Important Changes to Existing Functionality

IG 5.5.2

The following functionality is changed in IG 5.5.2:

- There are no important changes in functionality in this release.

IG 5.5.1

The following functionality is changed in IG 5.5.1:

- There are no important changes in functionality in this release.

IG 5.5

The following functionality is changed in IG 5.5:

Support for Java 7

Support for Java 7 has been removed. Before you update to IG 5.5, install the latest version of Java 8.

If you are using IG on Tomcat with SSL enabled, use OpenJDK 1.8.0_121 or later versions to prevent mismatch between client side ciphers and server side ciphers.

Default cookie name is `IG_SESSIONID`

Most web containers use `JSESSIONID` as the default cookie name. To prevent invalid session IDs when a protected application uses the same cookie name as the IG web container, IG now uses `IG_SESSIONID` as its default cookie name.

Configuration of Jetty for HTTPS

The way to configure HTTPS for Jetty has changed in Jetty 9.4.

For information about Jetty 9.4, see "Configuring Jetty For HTTPS (Server-Side)" in the *Gateway Guide*. For general information about Jetty and HTTPS, see <http://www.eclipse.org/jetty/documentation/current/configuring-ssl.html#configuring-sslcontextfactory>.

Support for "scope" in Dynamic Client Registration

As required by RFC 7591, *OAuth 2.0 Dynamic Client Registration Protocol*, the `metadata` property of `OAuth2ClientFilter` now supports `scope`.

Dynamic client registration with versions of AM earlier than 5.5 must use the `scopes` property.

Dynamic client registration with AM 5.5 can use the `scopes` or `scope` property.

For the option to dynamically register with a wider range of identity providers, you can use both `scope` and `scopes` at the same time.

3.2. Deprecated Functionality

The following functionality is deprecated in IG 5.5. Deprecation is defined in "ForgeRock Product Interface Stability" in the *Configuration Reference*.

IG 5.5.2

- No functionality has been deprecated in this release, other than those identified in IG 5.5.

IG 5.5.1

- No functionality has been deprecated in this release, other than those identified in IG 5.5.

IG 5.5

HeapClientRegistrationRepository

The class `HeapClientRegistrationRepository` is deprecated and will be removed in a future release. Declare client registrations in the `registrations` attribute of `OAuth2ClientFilter`.

Deprecated Configuration Settings

Configuration Object	Deprecated Settings	Newer Evolving Settings
<code>OAuth2ResourceServerFilter</code>	<code>cacheExpiration</code> (deprecated in IG 5.5.1, and the values of <code>zero</code> and <code>unlimited</code> are not supported)	Replaced by <code>cache</code> and its sub-properties <code>enabled</code> , <code>defaultTimeout</code> , and <code>maxTimeout</code> . If <code>cacheExpiration</code> is configured and <code>cache</code> is not configured, the

Configuration Object	Deprecated Settings	Newer Evolving Settings
		<p>cache is enabled and the value of <code>cacheExpiration</code> is used as <code>maxTimeout</code>.</p> <p>The following values for <code>cacheExpiration</code>, supported in previous releases, are not supported in this release: <code>zero</code>, <code>unlimited</code>.</p> <p>For more information, see <code>OAuth2ResourceServerFilter(5)</code> in the <i>Configuration Reference</i>.</p>
<code>OAuth2ResourceServerFilter</code>	<code>tokenInfoEndpoint</code> and <code>providerHandler</code>	<p>Replaced by configuration properties of <code>OpenAmAccessTokenResolver</code>, <code>TokenIntrospectionAccessTokenResolver</code>, and <code>ScriptableAccessTokenResolver</code>.</p> <p>For more information, see <code>OAuth2ResourceServerFilter(5)</code> in the <i>Configuration Reference</i>.</p>
<code>OAuth2ClientFilter</code>	<code>tokenEndpointUseBasicAuth</code>	<p>Replaced by <code>tokenEndpointAuthMethod</code>.</p> <p><code>"tokenEndpointAuthMethod": "client_secret_post"</code> is equivalent to <code>"tokenEndpointUseBasicAuth": false</code></p> <p><code>"tokenEndpointAuthMethod": "client_secret_basic"</code> is equivalent to <code>"tokenEndpointUseBasicAuth": true</code></p>

3.3. Removed Functionality

The following functionality is removed in IG 5.5. Removed is defined in "ForgeRock Product Interface Stability" in the *Configuration Reference*.

IG 5.5.2

- No features or functionality have been removed in this release.

IG 5.5.1

- No features or functionality have been removed in this release.

IG 5.5

Support for UMA 1

Support for UMA 1.x is removed in this release. Features and functionality have been upgraded to support new UMA standards.

Finalize Method Removed for HTTP messages

To reduce memory consumption, the `finalize()` method has been removed for HTTP messages (requests and responses). Consequently, requests are not automatically closed at garbage collection time.

Consider the following compatibility points:

- After creating a new request object, you must now explicitly close it after use. For example, the following Java code was used in the previous release:

```
ThrottlingRate rate = datasource.lookup(new RootContext(), new Request()).get();
```

In this release, the equivalent Java code includes a final `close` operation:

```
ThrottlingRate rate = datasource.lookup(new RootContext(), request)
    .thenAlways(request::close)
    .get();
```

- In scripts, the `client` binding automatically closes the request that is provided as a parameter. Therefore, it is not necessary to manually close the request for scripts.

After the request is automatically closed, the request entity is empty and can't be accessed. Response callbacks that try to access the request entity will fail.

You can workaroud this behavior in the following ways:

- Keep the request open by using the `client.sendNoClose()` method instead of `client.send()`. This method to prevents closure of requests after send. If you use this method, remember to manually close the request.
- Access the request entity before the request is closed, for example by including the `request.entity.string` assignment before calling the `client.send()` with the request.

Removed Configuration Settings

Configuration Object	Removed Settings	Newer Evolving Settings
UmaService	<code>clientId</code> and <code>clientSecret</code>	Not replaced. IG uses the PAT to create an UMA resource. For information, see "Supporting UMA Resource Servers" in the Gateway

Configuration Object	Removed Settings	Newer Evolving Settings
		<i>Guide</i> and <i>UmaService(5)</i> in the <i>Configuration Reference</i> .

Chapter 4

Fixes, Limitations, and Known Issues

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

4.1. Key Fixes

Key Fixes in IG 5.5.2

The following important issues have been fixed in IG 5.5.2:

- COMMONS-220: Add support for SameSite Cookies to CHF
- COMMONS-511: Add support for SameSite=None Cookies
- OPENIG-4048: Update Jackson Databind to 2.10

Key Fixes in IG 5.5.1

The following important issues have been fixed in IG 5.5.1:

- OPENIG-3256: Getting user_info on google fails because of returned different scopes than expected
- OPENIG-3226: StaticFilterRequest: request leak
- OPENIG-3219: When using scan feature in logback.xml the ig.instance.dir property is lost on reload
- OPENIG-3187: Backport httpOnly change in HTTP Session cookie to IG 5.5.x
- OPENIG-3159: Backport httpOnly change in JWT Session cookie to IG 5.5.x
- OPENIG-2571: OAuth2ResourceServerFilter requireHttps=true applies to rebased request URI
- OPENIG-2243: AM 6 default CSRF Protection switch breaks Policy Enforcement Filter
- OPENIG-2004: OAuth2ResourceServerFilter cache configuration can lead to unexpected results if tokens expire early

Key Fixes in IG 5.5

The following important issues have been fixed in IG 5.5:

- OPENIG-1876: SingleSignOnFilter throws NullPointerException if cookieName config item is not provided
- OPENIG-1674: UMA examples might not work with Chrome and Safari
- OPENIG-1152: Facebook Social Authentication not working when OpenAM is proxied behind OpenIG
- OPENIG-1924: Investigate removing finalize() method implementation from CHF classes

4.2. Limitations

IG 5.5.2

- OPENIG-221: Cannot specify which certificate to present to server if server requires mutual authentication in https
- OPENIG-234: Federation doesn't work if we used incomplete user in IDP
- OPENIG-291: Class cast exception when using SAML federation & policy agent together
- OPENIG-458: CookieFilter is not JwtSession compatible
- OPENIG-813: auditService : fileRotation may overwrite existing audit file
- OPENIG-1557: UI: Unable to deploy route when custom router is configured
- OPENIG-3273: Persists UMA Shares
- OPENIG-3274: IG Scripts Can Access Anything in Their Environment
- OPENIG-3275: SamlFederationHandler Doesn't Support Filtering

IG 5.5.1

- There are no limitations in functionality in this release.

IG 5.5

The following important limitations are included in this release:

Persists UMA Shares (OPENIG-3273)

Shared resources cannot be persisted when IG restarts. They must be shared each time that IG restarts. For more information, see "*Supporting UMA Resource Servers*" in the *Gateway Guide*.

Cannot Use Custom `config.json` in IG Studio (OPENIG-1557)

When a customized `config.json` is configured in IG Studio, IG Studio cannot deploy routes.

PolicyEnforcementFilter Cache Can Become Outdated

The `PolicyEnforcementFilter` can keep policy decisions in the cache after a user has logged out and the session has become invalid. Because the `PolicyEnforcementFilter` does not listen to AM notifications, it is not aware that a user has logged out, and is therefore not aware that the policy decision should be evicted from the cache.

Log File of Audit Events Can be Overwritten (OPENIG-813)

The log file of audit events can be overwritten when the log file is rotated.

When `CsvAuditEventHandler` is used to log audit events, the log file is overwritten if it is rotated before the file suffix, `rotationFileSuffix`, changes. By default, `rotationFileSuffix` is defined as a date in the format `_yyyy-MM-dd`.

Log files are rotated when one of the following limits is reached: `maxFileSize`, `rotationInterval`, or `rotationTimes`.

Set the log rotation parameters so that the log is not likely to rotate before `rotationFileSuffix` changes.

For Mutual Authentication in HTTPS Cannot Specify Which Certificate to Present (OPENIG-221)

IG can check server certificates for HTTPS. However, for mutual authentication, the client certificate must be the first certificate in the `KeyStore`.

IG Scripts Can Access Anything in Their Environment (OPENIG-3274)

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

SamlFederationHandler Doesn't Support Filtering (OPENIG-3275)

The `SamlFederationHandler` does not support filtering. Do not use a `SamlFederationHandler` as the handler for a `Chain`.

More generally, do not use this handler when its use depends on something in the response. The response can be handled independently of IG, and can be `null` when control returns to IG. For example, do not use this handler in a `SequenceHandler` where the `postcondition` depends on the response.

4.3. Known Issues

IG 5.5.2

- OPENIG-659: `CryptoHeaderFilter` - error on handling header value with incorrect length
- OPENIG-3221: OpenIG is decoding special character ' while sending to the backend which is causing issues

- OPENIG-3403: ContentTypeHeader quoted directives should be maintained

IG 5.5.1

- OPENIG-3221: OpenIG is decoding special character ' while sending to the backend which is causing issues
- OPENIG-3113: Not possible to use token substitutions within a monitor decorator of a Route

IG 5.5

- OPENIG-2004: OAuth2ResourceServerFilter cache configuration can lead to unexpected results if tokens expire early
- OPENIG-1628: Script update referenced in route, not taken into account
- OPENIG-1557: UI: Unable to deploy route when custom router is configured
- OPENIG-1325: Cannot specify realm in UmaService
- OPENIG-816: The UmaResourceServerFilter returns with wrong as_uri
- OPENIG-813: auditService : fileRotation may overwrite existing audit file
- OPENIG-659: CryptoHeaderFilter - error on handling header value with incorrect length
- OPENIG-458: CookieFilter is not JwtSession compatible
- OPENIG-291: Class cast exception when using SAML federation & policy agent together
- OPENIG-234: Federation doesn't work if we used incomplete user in IDP
- OPENIG-221: Cannot specify which certificate to present to server if server requires mutual authentication in https
- OPENAM-9112: Audit logging outputs errors in debug log under high load

Chapter 5

Documentation Changes

The following table tracks changes to the documentation set following the release of IG 5.5:

Documentation Change Log

Date	Description
2020-04-15	Minor correction in routes for SAML with multiple service providers.
2019-11-21	Release of IG 5.5.2, maintenance release.
2019-05-28	Minor correction in SingleSignOnFilter.
2018-12-28	Release of IG 5.5.1, maintenance release.
2018-01-30	Noted that cached policy decisions remain in the cache even after a user logs out of OpenAM. For information, see <code>PolicyEnforcementFilter(5)</code> in the <i>Configuration Reference</i> .
2017-10-31	<p>Release of IG 5.5:</p> <ul style="list-style-type: none"> • The Getting Started Guide has been added to describe how to install and configure IG. • The <i>ForgeRock Identity Platform Devops Guide</i> provides instructions for deploying IG using DevOps techniques, where an IG runs in Kubernetes. See Deploying the IG Example . <p>The Kubernetes examples provided in GitHub , and the description of how to use them in the Deployment Guide have been replaced with links to the <i>ForgeRock Identity Platform Devops Guide</i>.</p>

Chapter 6

Getting Support

This chapter includes information and resources for IG and ForgeRock support.

6.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

6.2. How to Report Problems or Provide Feedback

If you find issues or reproducible bugs, 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
- Description of the environment, including the following information:
 - Machine type
 - Operating system and version
 - Web server or container and version
 - Java version
 - Patches or other software that might affect the problem
- Steps to reproduce the problem

- Relevant access and error logs, stack traces, and core dumps

6.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see <https://www.forgerock.com>.

ForgeRock has staff members around the globe who support our international customers and partners. For details on ForgeRock's support offering, including support plans and service level agreements (SLAs), visit <https://www.forgerock.com/support>.