# Release Notes

/ ForgeRock Identity Gateway 5

Latest update: 5.0.0

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 © 2012-2017 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. This license is available with a FAQ at: http://scripts.sil.org/OFL

# Table of Contents




Copyright © 2012-2017 ForgeRock AS. All rights reserved.

# Preface

ForgeRock Identity Platform™ is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

The platform includes the following components that extend what is available in open source projects to provide fully featured, enterprise-ready software:

- ForgeRock Access Management (AM)
- ForgeRock Identity Management (IDM)
- ForgeRock Directory Services (DS)
- ForgeRock Identity Gateway (IG)
- ForgeRock Identity Message Broker (IMB)


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

Chapter 1
# What's New in This Release

OpenIG 5 provides many new features and improvements.

## 1.1. New Features

This release of OpenIG includes the following new features:

**OpenIG Studio**

OpenIG Studio is a new tool to help you build and deploy your OpenIG configuration through a user interface.

Through OpenIG Studio, you can create routes to authenticate and authorize users' access to protected applications, and throttle the rate of requests.

For information, see Section 12.4, "Creating Routes Through OpenIG Studio " in the *Gateway Guide*.

**Mutable and Immutable Modes**

OpenIG now provides a development mode and a production mode to make it easy to develop and then secure your configuration:

- In development mode, by default all endpoints are exposed and accessible. This mode is also called *mutable*.

  In development mode, you can use the `/routes` endpoint to read, add, edit, delete, and list routes in the OpenIG configuration. For examples, see Section 12.3, " Creating and Editing Routes Through Common REST " in the *Gateway Guide*.

  Use development mode to evaluate or demo OpenIG, or to develop configurations on a single instance. Development mode is not suitable for production.

- In production mode, the `/routes` endpoint is not exposed or accessible, and other endpoints are exposed according to the configuration of the `ApiProtectionFilter`. If there is no `ApiProtectionFilter`, other endpoints are exposed only to the loopback address. This mode is also called *immutable*.

  After creating your configurations in development mode, switch to production mode to test OpenIG, to run OpenIG in pre-production or production, or to run multiple instances of OpenIG.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

The default mode is development. For information about switching to production mode, see Section 3.8, "Making the Configuration Immutable" in the *Gateway Guide*.

**Support for Step-up Authentication**

Step-up authentication is now supported in the following ways:

- OpenIG can respond to authentication-level advice provided when a policy decision is denied.
- The `PolicyEnforcementFilter` has a new property `failureHandler`, which can be configured to recover and respond to advice provided when a policy decision is denied.

After a policy decision, OpenIG continues to process requests as follows:

- If the request is allowed, processing continues.
- If the request is denied with advice, OpenIG checks whether it can respond to the advice. If OpenIG can respond to the advice, it processes the advice.
- If the request is denied without advice, or if OpenIG cannot respond to the advice, OpenIG forwards the request to a `failureHandler` declared in the `PolicyEnforcementFilter`. If there is no `failureHandler`, OpenIG returns a 403 Forbidden.
- If an error occurs during the process, OpenIG returns 500 Internal Server Error.

For an example configuration for step-up authentication, see the `failureHandler` property of PolicyEnforcementFilter(5) in the *Configuration Reference*.

**Support for Single Sign-On With OpenAM**

The `SingleSignOnFilter` has been added to support authentication with OpenAM before processing requests. The filter tests for the presence and validity of an SSO token in the cookie header of a request. If the SSO token is not present, or if it is empty or invalid, the filter redirects the user agent to the OpenAM login page for authentication.

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

**Configuration Parameters as Property Variables and Inherited Across the Router**

Configuration parameters, such as host names, port numbers, and directories, can be declared as property variables in the OpenIG configuration or in an external JSON file. The variables can then be used in expressions in routes and in `config.json` to set the value of configuration parameters.

Properties can be inherited across the router, so a property defined in `config.json` can be used in any of the routes in the configuration.

Storing the configuration centrally and using variables for parameters that can be different for each installation makes it easier to deploy OpenIG in different environments without changing a single line in your route configuration.

For more information, see Properties(5) in the *Configuration Reference*.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

### Implicit Object `openig` Gives Access to Environment

When expressions are evaluated, they now access the environment through the implicit object `openig`.

For more information, see "Configuration and Runtime Expressions" in the *Configuration Reference*.

### Chain of Filters

`ChainOfFilters` has been added to dispatch a request to an ordered list of filters that does not end with a handler. Use this filter to assemble a list of filters into a single filter that you can then use in different places in the configuration.

For more information, see ChainOfFilters(5) in the *Configuration Reference*.

### Conditional Filter

`ConditionalFilter` has been added to make it easy to use or skip a filter depending on whether a condition is met (OPENIG-1138).

For more information, see ConditionalFilter(5) in the *Configuration Reference*.

### Scriptable Filters and Handlers Support Multiline Scripts

In scriptable filters and handlers, the property `"source"` can now be written as a string or array of strings, to make it more readable. The route is valid JSON, and can be deployed as a file or as a CREST resource.

Before this release, a route with a property `"source"` that contained line breaks was invalid JSON, and was tolerated only when deployed as a file.

For an example of `"source"` written as an array of strings, see "Example of a Scriptable Throttling Policy" in the *Configuration Reference*.

### Decorating Individual Uses of Named Filters and Handlers

When a named filter or handler is configured in `config.json` or in the heap, it can be used many times in the configuration. You can now use a delegate to decorate each use of a named filter or handler individually.

This new feature allows you to decorate a named filter or handler differently each time you use it in the configuration.

For more information, see Section 3.4, " Decorating Individual Uses of a Named Filter or Handler " in the *Configuration Reference*.

### Audit Event Handlers

Support has been added for the JMS Audit Handler and JSON Audit Handler For information, see JmsAuditEventHandler(5) in the *Configuration Reference* and JsonAuditEventHandler(5) in the *Configuration Reference*.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

**API Descriptors**

The following endpoints now serve API descriptors at runtime: `../info`, `../router-name/routes`, `../umaservice-name/share`, and `../routeId/monitoring`.

For information, see Section 1.10, "Understanding OpenIG APIs With API Descriptors" in the *Gateway Guide*.

**REST Endpoint for Server and Build Information**

The product version and build information for a running instance of OpenIG can now be retrieved from the `/api/info` endpoint. When OpenIG is set up as described in Chapter 2, "*Getting Started*" in the *Gateway Guide*, you can access the information at http://openig.example.com:8080/openig/api/info.

## 1.2. Product Improvements

This release of OpenIG includes the following improvements:

**Routes Reloaded Automatically Into the Configuration**

When a route has been updated, by default it is reloaded automatically in the OpenIG configuration. Before this release, is was necessary to access the route to load it into the OpenIG configuration.

The scanning interval of `Router` can now be configured with a duration. Before this release, it could be configured only with an integer that defined a number of seconds.

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

**Policy Enforcement Filter Cache Can Be Disabled**

To force OpenIG to apply for a new policy decision for every request, you can now disable the cache in the `PolicyEnforcementFilter`.

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

**Addition of a Domain for JWT Cookies**

The property `cookieDomain` has been added to `JwtSession`.

When the domain is specified, a JWT cookie can be accessed from different hosts in that domain. When the domain is not specified, the JWT cookie can be accessed only from the host where the cookie was created.

The `sharedSecret` property specifies the key used to sign and verify JWTs. If this property is not specified, random data is generated as the key, and the OpenIG instance can verify only the sessions it has created.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

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

**Integer and Boolean Functions for Expressions**

The following functions have been added for expressions: `integer`, `boolean`, `fileToUrl`, and `pathToUrl`.

For more information, see Functions(5) in the *Configuration Reference*

**Unit of Time for `TimerDecorator` Defined by Parameter**

The property `timeUnit` has been added to `TimerDecorator`, to make it possible to define the unit of time used by the decorator.

For more information, see TimerDecorator(5) in the *Configuration Reference*

**Addition of `µs` to the `Duration` class**

The unit `µs` has been added to the `Duration` class as an abbreviation for microseconds.

**Home Page for the Sample Application**

A mockup web application is provided for testing OpenIG configurations. A home page has been added to this sample application.

Requests can access the home page without the need log in to the sample application. For information, see Section 2.3, "Install the Sample Application" in the *Gateway Guide*.

## 1.3. 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 more information on ForgeRock's security advisory policy, click the following link: http://www.forgerock.com/services/security-policy/.

The following security advisory is about vulnerabilities in this release:

- OpenIG Security Advisory #201606


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

Chapter 2

# Before You Install

This chapter covers requirements for running OpenIG.

**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 OpenIG Software

Download the following product software from the ForgeRock BackStage download site:

- OpenIG .war file, `IG-5.0.0.war`
- Mockup web application for testing OpenIG configurations, `IG-doc-samples-5.0.0.jar`

## 2.2. JDK Version

OpenIG runs with the following JDKs:

- Oracle JDK 7 or 8
- OpenJDK 1.8

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

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

## 2.3. Web Application Containers

OpenIG runs in the following web application containers:

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


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

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

OpenIG requires Servlet 3.0 or later.

For details on setting up your web application container see Section 3.1, "Configuring Deployment Containers" in the *Gateway Guide*.

## 2.4. OpenAM Features

The following OpenIG features are supported with OpenAM 13.5.0 and AM 5:

- OpenAM policy enforcement, as described in Chapter 6, "*Enforcing Policy Decisions and Supporting Session Upgrade*" in the *Gateway Guide*
- OpenID Connect dynamic registration and discovery, as described in Section 9.8, "Using OpenID Connect Discovery and Dynamic Client Registration" in the *Gateway Guide*
- User Managed Access, as described in Chapter 11, "*Supporting UMA Resource Servers*" in the *Gateway Guide*
- Token transformation, as described in Chapter 10, "*Transforming OpenID Connect ID Tokens Into SAML Assertions*" in the *Gateway Guide*.

## 2.5. OpenAM Policy Agents

When installing an OpenAM policy agent in the same container as OpenIG, use 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 OpenIG and for the Java EE Policy Agent that you install alongside OpenIG.

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


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

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

This release of OpenIG includes the following important changes:

**Update Required in Scripts that Authenticate to DS 5.0.0**

DS 5.0.0 has been refactored and some APIs have changed:

- The `org.forgerock.opendj.ldap.requests` and `org.forgerock.opendj.ldap.responses` packages have been renamed to `org.forgerock.opendj.ldap.messages`
- The following methods and class names have been renamed for consistent use of camel case:
  - The `DN` class has been renamed to `Dn`
  - The `ModifyDNRequest` class has been renamed to `ModifyDnRequest`
  - The `Requests.newModifyDNRequest()` factory method has been renamed to `Requests.newModifyDnRequest()`

If OpenIG uses scripts to authenticate to DS 5.0.0, adapt the scripts according to the changes listed in the following tables:

*Table 3.1. Static Imports*

| OpenDJ 3.5 and Earlier Releases | DS 5.0.0 |
|---|---|
| `org.forgerock.opendj.ldap.requests.Requests.newAddRequest` | `org.forgerock.opendj.ldap.messages.Requests.newAddRequest` |
| `org.forgerock.opendj.ldap.requests.Requests.newCompareRequest` | `org.forgerock.opendj.ldap.messages.Requests.newCompareRequest` |
| `org.forgerock.opendj.ldap.requests.Requests.newDeleteRequest` | `org.forgerock.opendj.ldap.messages.Requests.newDeleteRequest` |
| `org.forgerock.opendj.ldap.requests.Requests.newModifyDNRequest` | `org.forgerock.opendj.ldap.messages.Requests.newModifyDnRequest` |


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

| OpenDJ 3.5 and Earlier Releases | DS 5.0.0 |
|---|---|
| `org.forgerock.opendj.ldap.requests.Requests .newModifyRequest` | `org.forgerock.opendj.ldap.messages.Requests .newModifyRequest` |
| `org.forgerock.opendj.ldap.requests.Requests .newSearchRequest` | `org.forgerock.opendj.ldap.messages.Requests .newSearchRequest` |
| `org.forgerock.opendj.ldap.requests.Requests .newSimpleBindRequest` | `org.forgerock.opendj.ldap.messages.Requests .newSimpleBindRequest` |

*Table 3.2. Other Imports*

| OpenDJ 3.5 and Earlier Releases | DS 5.0.0 |
|---|---|
| `import org.forgerock.opendj.ldap.DN;` | `import org.forgerock.opendj.ldap.Dn;` |
| `import org.forgerock.opendj.ldap.requests .AddRequest;` | `import org.forgerock.opendj.ldap.messages .AddRequest;` |
| `import org.forgerock.opendj.ldap.requests .BindRequest;` | `import org.forgerock.opendj.ldap.messages .BindRequest;` |
| `import org.forgerock.opendj.ldap.requests .CompareRequest;` | `import org.forgerock.opendj.ldap.messages .CompareRequest;` |
| `import org.forgerock.opendj.ldap.requests .DeleteRequest;` | `import org.forgerock.opendj.ldap.messages .DeleteRequest;` |
| `import org.forgerock.opendj.ldap.requests .ModifyDNRequest;` | `import org.forgerock.opendj.ldap.messages .ModifyDnRequest;` |
| `import org.forgerock.opendj.ldap.requests .ModifyRequest;` | `import org.forgerock.opendj.ldap.messages .ModifyRequest;` |
| `import org.forgerock.opendj.ldap.requests .Request;` | `import org.forgerock.opendj.ldap.messages .Request;` |
| `import org.forgerock.opendj.ldap.requests .SearchRequest;` | `import org.forgerock.opendj.ldap.messages .SearchRequest;` |
| `import org.forgerock.opendj.ldap.responses .BindResult;` | `import org.forgerock.opendj.ldap.messages .BindResult;` |
| `import org.forgerock.opendj.ldap.responses .CompareResult;` | `import org.forgerock.opendj.ldap.messages .CompareResult;` |
| `import org.forgerock.opendj.ldap.responses .Result;` | `import org.forgerock.opendj.ldap.messages.Result;` |
| `import org.forgerock.opendj.ldap.responses .SearchResultEntry;` | `import org.forgerock.opendj.ldap.messages .SearchResultEntry;` |
| `import org.forgerock.opendj.ldap.responses .SearchResultReference;` | `import org.forgerock.opendj.ldap.messages .SearchResultReference;` |

For an example script that authenticates against an LDAP server, see Section 14.4, "Scripting LDAP Authentication" in the *Gateway Guide*.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

### OpenIG Class `Logger` Replaced by SLF4J Class `Logger`

The OpenIG class `Logger` has been replaced by the SLF4J class `Logger`. The behavior of Groovy scripts that worked with the OpenIG class `Logger` can be affected. Review references to `ConsoleLogSink`, `FileLogSink`, and `Slf4jLogSink` from scripts used in the `ScriptableFilter`, `ScriptableHandler`, and `ScriptableThrottlingPolicy`.

For information about the SLF4J class `Logger`, see http://www.slf4j.org/apidocs/org/slf4j/Logger.html.

### Configuration File for Administrative Requests

The file `$HOME/.openig/config/admin.json` has been added as the entry point for administrative requests. The entry point for gateway requests is still `$HOME/.openig/config/config.json`.

Before this release the `ApiProtectionFilter` was configured in `config.json`. It is now configured in `admin.json`

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

### In Groovy scripts, the Response constructor for a new Response object requires a Status

Before this release, constructions like the following were allowed:

```
Response response = new Response
response.status = Status.OK
```

In this release, that construction must be written as follows:

```
Response response = new Response(Status.OK)
```

### Attributes of a SAML assertion can contain one or more values

The attributes of a SAML assertion can contain one or more values. Before this release, only the first value was made available. Now, all values are made available as a list of strings. Even if an attribute contains a single value, it is made available as a list of strings.

Update scripts and expressions that use SAML assertions so that they refer to the correct value in the list of strings. Even if the list contains only one value, include the braces `[ ]` to refer to that value. For example, use the following code to refer to the value of the username and password attributes of a SAML assertion:

```
"form": {
  "username": [
    "${session.username[0]}"
  ],
  "password": [
    "${session.password[0]}"
  ]
}
```


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

### Changes to the PolicyEnforcementFilter

The following changes have been made in the `PolicyEnforcementFilter`:

- By default, policy decisions are not cached.
- Policy decisions that contain advices are never cached.
- The `cache` subproperty of `cacheMaxExpiration` has been removed.

  To configure caching for policy decisions, use the new `cache` property, with subproperties `enabled`, `defaultTimeout`, and `maxTimeout`. For an example, see the `cache` property of PolicyEnforcementFilter(5) in the *Configuration Reference*.

- The `target` property has been removed. Before this release, attributes and advices returned by a policy decision were stored in the location defined by the `target` attribute. They are now stored in the context `${contexts.policyDecision}`.

### Token Transformation Filter Property `target` Removed

The `TokenTransformationFilter` property `target` has been removed. Before this release, SAML 2.0 assertions were made available to downstream handlers through the location defined by the `target` attribute. They are now made available through the context `${contexts.sts}`.

### Session Cookies Created by Default When Using `JwtSession`

By default, cookies created when using `JwtSession` are now session cookies. OpenIG does not specify an expiry date for session cookies. The user-agent is responsible for deleting them when it considers that a session is finished (for example, when the browser is closed).

Before this release, cookies created when using `JwtSession` were always persistent cookies, with an expiry date based on `sessionTimeout`.

`JwtSession` has a new property, `persistentCookie`. Set this property to `true` to create persistent cookies when using `JwtSession`, which is the behavior before this release.

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

### Failure Handling in `OAuth2ClientFilter`

When the OAuth 2.0 Resource Server denies access to a resource, the `OAuth2ClientFilter` can invoke the failure handler only if the error response contains a WWW-Authenticate header (meaning that there was a problem with the OAuth 2.0 exchange). Before this release, the filter invoked the failure handler for a wider range of errors.

If the value of the WWW-Authenticate header is `invalid_token`, the OAuth2ClientFilter first tries to refresh the token and replay the request. Before this release, the filter tried to refresh the token only when the response also had a `401 Unauthorized`.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

**`temporaryStorage` is no longer an implicit property of a heap object**

The property `temporaryStorage` is no longer an implicit property of a heap object. In the ClientHandler, `temporaryStorage` is a new configuration property. For information, see ClientHandler(5) in the *Configuration Reference*.

**OAuth2ResourceServerFilter uses ForgeRockClientHandler as the default handler.**

To facilitate issue tracking, the default handler for the OAuth2ResourceServerFilter property `providerHandler` is now the ForgeRockClientHandler. Before this release, it was the default ClientHandler. For information, see OAuth2ResourceServerFilter(5) in the *Configuration Reference*.

**Arguments of a scriptable object cannot access runtime properties**

The values for script arguments that are defined as configuration expressions cannot refer to `context`, `request`, `contexts`, `session`, or `attributes`.

Instead, the variables can be accessed directly within the script. For maintenance, it easier to maintain the variables inside the script, with their usage context, instead of decoupling them from the script.

The arguments are evaluated once, at configuration time, instead of at every request.

## 3.2. Deprecated Functionality

This section lists deprecated functionality. Deprecation is defined in Section A.2, "ForgeRock Product Interface Stability" in the *Configuration Reference*.

- Support for Java 7 is deprecated and will be removed in the next 5.5 release.

  When upgrading to the current release, also move to Java 8 in order to be prepared for pending removal of support for Java 7.

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

*Table 3.3. Deprecated Configuration Settings*

| Configuration Object | Removed Settings | Newer Evolving Settings |
|---|---|---|
| `OAuth2ClientFilter` | `tokenEndpointUseBasicAuth` | Replaced by `tokenEndpointAuthMethod`.<br><br>`"tokenEndpointAuthMethod": "client_secret_post"` is equivalent to `"tokenEndpointUseBasicAuth": false` |


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

| Configuration Object | Removed Settings | Newer Evolving Settings |
|---|---|---|
| | | `"tokenEndpointAuthMethod": "client_secret_basic"` is equivalent to `"tokenEndpointUseBasicAuth": true` |

## 3.3. Removed Functionality

This section lists removed functionality. Removed is defined in Section A.2, "ForgeRock Product Interface Stability" in the *Configuration Reference*.

- The following classes are removed in this release: `ConsoleLogSink`, `FileLogSink`, `Slf4jLogSink`. SLF4J is now provided in OpenIG, allowing you to define different logging behavior for routes and third-party dependencies.
- The convenience class `GenericHeapObject` is removed in this release.

*Table 3.4. Removed Configuration Settings*

| Configuration Object | Removed Settings | Newer Evolving Settings |
|---|---|---|
| `AuditDecorator` | Entire object | Replaced by the ForgeRock common audit framework. For information, see Chapter 15, "*Auditing and Monitoring*" in the *Gateway Guide*. |
| `CaptureDecorator` | `captureExchange` | New name: `captureContext` |
| | `logSink` | Logging is now provided by SLF4J logging. |
| `ClientHandler` | `httpClient` | All former `HttpClient` configuration attributes must be set in `ClientHandler` instead.<br><br>Scriptable handlers and scriptable filters must use the `clientHandler` attribute to refer to a handler. |
| `GatewayHttpApplication` | `handlerObject` | `handler` |
| | Removed format: `"heap": { "objects": [ configuration object, ... ] }` | New format: `"heap": [ configuration object, ... ]` |
| `MonitorEndpointHandler` | Entire object | Replaced by the ForgeRock common audit framework. For information, see Chapter 15, "*Auditing and Monitoring*" in the *Gateway Guide*. |


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

| Configuration Object | Removed Settings | Newer Evolving Settings |
|---|---|---|
| `OAuth2ClientFilter` | `"registration": ClientRegistration reference` | Replaced by `"registrations": [ ClientRegistration reference(s) ]`. |
| `OAuth2ResourceServerFilter` | `enforceHttps` | New name: `requireHttps` |
| | `httpHandler` | New name: `providerHandler` |
| | `requiredScopes` | New name: `scopes` |
| `PolicyEnforcementFilter` | `policiesHandler`, using `ClientHandler` as default. | Replaced by `amHandler`, using `ForgeRockClientHandler` as default. |
| | `cacheMaxExpiration` | Replaced by `cache`, using `enabled`, `default`, and `maxTimeout`. |
| | `target` | Attributes and advices returned by a policy decision are stored in the `${contexts.policyDecision}` context. |
| `RedirectFilter` | Entire object | Replaced by `LocationHeaderFilter` |
| `Route` | Removed format: `"heap": { "objects": [ configuration object, ... ] }` | New format: `"heap": [ configuration object, ... ]` |
| `ThrottlingFilter` | `partitionKey` | Replaced by `requestGroupingPolicy` |
| `TokenTransformationFilter` | `target` | SAML 2.0 assertions are made available to downstream handlers through the context `${contexts.sts}`. |


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

Chapter 4

# Fixes, Limitations, and 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 5.

## 4.1. Key Fixes

This release of OpenIG fixes the following important issues:

- OPENIG-1632: UMA scenario of gateway Guide does not work with OpenAM 13.5.0
- OPENIG-1536: Infinite loop when dumping context
- OPENIG-1491: OAuth2: expires_in field is recommended, not mandatory
- OPENIG-1367: Scriptable object's arguments should not have access to runtime properties
- OPENIG-1349: PolicyEnforcementFilter: Cannot use an expression to define a header in the "environment" property
- OPENIG-1257: The PolicyEnforcementFilter does not recover from problems authenticating with OpenAM
- OPENIG-1227: PolicyEnforcementFilter : after getting a new pep token, OpenIG requests a policy evaluation without providing the resources & subject
- OPENIG-1220: matches() function for a query throws NPE when the request does not contain any query
- OPENIG-983: Keystore can be declared inline
- OPENIG-953: ClientRegistration defined in heap cannot be referenced by OAuth2ClientFilter

## 4.2. Limitations

This release of OpenIG includes the following limitations:


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

### For OpenIG Studio, Custom `config.json` Must Contain Main Router Named `_router`

OpenIG Studio deploys and undeploys routes through a main router named `_router`, which is the name of the main router in the default configuration. If you use a custom `config.json`, make sure that it contains a main router named `_router`.

For information, see Section 12.4, "Creating Routes Through OpenIG Studio " in the *Gateway Guide*.

### `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 OpenAM 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

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, Client Certificate Must Be First in KeyStore

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 `ClientHandler` keystore.

### OpenIG Scripts Can Access Anything in Their Environment

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.

### `SamlFederationHandler` Doesn't Support Filtering

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 OpenIG, and can be `null` when control returns to OpenIG. For example, do not use this handler in a `SequenceHandler` where the `postcondition` depends on the response.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

# 4.3. Known Issues

This release of OpenIG includes the following known issues:

- OPENIG-1674: UMA examples might not work with Chrome and Safari
- 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-1152: Facebook Social Authentication not working when OpenAM is proxied behind OpenIG
- OPENIG-910: ScriptableFilter : Get error `Cannot execute script` with groovy scripts previously working
- 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-322: Cannot access both an OpenAM (self-signed) and a Google HTTPS endpoint
- 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


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

# Chapter 5
# Documentation Changes

This chapter describes important changes made to the documentation set.

This release of OpenIG includes the following changes to the documentation:

- The Deployment Guide has been added to describe how to deploy basic and customized configurations of OpenIG through Docker. To help you prepare for production deployments, it describes best practices for managing the secret and public configuration parameters that change from one deployment to another.

The following table tracks changes to the documentation set following the release of OpenIG 5:

*Table 5.1. Documentation Change Log*

| Date | Description |
|---|---|
| 2018-01-30 | Noted that cached policy decisions remain in the cache even after a user logs out of OpenAM. For information, see PolicyEnforcementFilter(5) in the *Configuration Reference*. |


Copyright © 2012-2017 ForgeRock AS. All rights reserved.

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, use the ForgeRock website.


Copyright © 2012-2017 ForgeRock AS. All rights reserved.