FORGEROCK®

Release Notes

/ ForgeRock Identity Gateway 6.1

Latest update: 6.1.0

Mark Craig
Joanne Henry

Copyright © 2012-2018 ForgeRock AS.

Abstract

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

Table of Contents

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.

FORGEROCK

Chapter 1
What's New

IG 6.1 provides new features and improvements.

1.1. New Features

This release of IG includes the following new features:

Proxy WebSocket Traffic

IG can now detect requests to upgrade from HTTP to the Websocket protocol, and create a dedicated tunnel to send and receive WebSocket traffic.

When you create a route in Studio, you can enable a new option to upgrade HTTP connections to WebSocket protocol.

To help with development, the sample app has been updated to include a WebSocket endpoint that exposes a simple WebSocket server.

> **Important**
>
> IG cannot proxy WebSocket traffic for TLS connections, or when it is running in the Jetty application container.

For more information, see "*Proxying WebSocket Traffic*" in the *Gateway Guide*, and the `websocket` property of ClientHandler(5) in the *Configuration Reference* or ReverseProxyHandler(5) in the *Configuration Reference*.

JwtBuilderFilter to Pass Identity or Other Runtime Info Downstream

A new filter, JwtBuilderFilter, collects data at runtime, packs it in a JSON Web Token (JWT), and places the resulting JWT into the JwtBuilderContext. When the JwtBuilderFilter is used with a HeaderFilter, it provides a flexible way for IG to pass identity or other runtime information to the protected application.

> **Important**
>
> The JWT created by JwtBuilderFilter can be signed but is not encrypted. Carefully consider the security of your configuration when using this filter.

For more information, see JwtBuilderFilter(5) in the *Configuration Reference* and JwtBuilderContext(5) in the *Configuration Reference*.

To help with development, the sample app has been updated to include a `/jwt` endpoint that displays the JWT and verifies its signature.

New Features in Freeform Studio

New features have been added to the technology preview of Freeform Studio to allow you to:

- Drag-and-drop filters and handlers onto the canvas.

- Add, reorder, or remove filters in a chain.

- Connect a start node to a chain or handler, and connect chains to handlers.

- Double-click on any node to edit it or rename it.

- Easily edit SingleSignOnFilters in a dedicated page that hides the JSON representation.

- Get feedback on structural errors in your route before you deploy it, by simply displaying the route configuration.

Routes created in Freeform Studio in IG 6.0 are automatically transitioned into JSON editor routes.

1.2. Product Improvements

This release of IG includes the following improvements:

Disable Capture

Instead of removing the decorator from the configuration, you can now configure the capture point `none` to disable capture.

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

Client Connection Pool timeToLive Is Configurable

You can now expire pooled connections after a fixed duration by setting a new property `connectionTimeToLive` in the ClientHandler and ReverseProxyHandler. To prevent the reuse of connections, set this property in routes for applications where the IP address (baseURI) is not stable or can change.

For more information, see ClientHandler(5) in the *Configuration Reference* and ReverseProxyHandler(5) in the *Configuration Reference*.

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 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 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-6.1.0.war`

- Web application for testing IG configurations, `IG-sample-application-6.1.0.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 8 or 8.5.x

- Jetty 9

- JBoss EAP 7

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
Eviction of entries from the AmService `sessionCache`, using WebSocket notifications from AM. For more information, see AmService(5) in the *Configuration Reference*.	AM 6, and AM 5.5 when the `AMCtxId` session property is whitelisted
AM password capture and replay, as described in "*Getting Login Credentials From AM*" in the *Gateway Guide*.	AM 5 and later
AM policy enforcement, as described in "*Enforcing Policy Decisions and Supporting Session Upgrade*" in the *Gateway Guide*.	AM 5 and later
OpenID Connect dynamic registration and discovery, as described in "Using OpenID Connect Discovery and Dynamic Client Registration" in the *Gateway Guide*.	OpenAM 13.5.x, and AM 5 and later
Token transformation, as described in "*Transforming OpenID Connect ID Tokens Into SAML Assertions*" in the *Gateway Guide*.	OpenAM 13.5.x, and AM 5 and later
User Managed Access 2.x, for IG 5.5, as described in "*Supporting UMA Resource Servers*" in the *Gateway Guide*.	AM 5.5 and later
User Managed Access 1.x, for IG 5 and earlier versions.	AM 5.1 and earlier
Single sign-on, as described in "About SSO Using the SingleSignOnFilter" in the *Gateway Guide*.	AM 5 and later
Cross-domain single sign-on, as described in "About CDSSO Using the CrossDomainSingleSignOnFilter" in the *Gateway Guide*.	AM 5.5 and later

Feature	Supported In AM Version
Capture and storage of AM session information, as described in SessionInfoFilter(5) in the *Configuration Reference*.	AM 5.5 and later
Capture and storage of AM user profile attributes, as described in UserProfileFilter(5) in the *Configuration Reference*.	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 or later. 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

This release of IG includes the following important change:

New Features in Freeform Studio

New features have been added to the technology preview of Freeform Studio. Routes created in Freeform Studio in IG 6.0 are automatically transitioned into JSON editor routes.

For information, see "New Features".

3.2. Deprecated Functionality

During IG upgrade, routes that were previously created in Studio are automatically transferred to the new version of IG. Where possible, IG replaces deprecated settings with the newer evolved setting. If IG needs additional information to upgrade the route, the route status becomes ⚠ Compatibility update required. Select the route and provide the requested information.

This section lists deprecated functionality. Deprecation is defined in "ForgeRock Product Interface Stability".

IG Route Monitoring Endpoint

The IG Route Monitoring Endpoint is deprecated in this release and will be removed in the next release. As a replacement, IG provides Prometheus Scrape Endpoint and Forgerock Common REST Monitoring Endpoint.

For more information, see "Prometheus Scrape Endpoint" in the *Gateway Guide*, and "Forgerock Common REST Monitoring Endpoint" in the *Gateway Guide*,

Support for .war File Delivery

The delivery of a .war file is deprecated in this release and may be removed in the next release.

Support AM Policy Agents

Support for the use of AM policy agents in password capture and replay is deprecated in this release.

By using CapturedUserPasswordFilter, you can get login credentials from AM without setting up an AM policy agent. For more information, see "*Getting Login Credentials From AM*" in the *Gateway Guide*, and CapturedUserPasswordFilter(5) in the *Configuration Reference*.

Deprecated Configuration Settings

Configuration Object	Deprecated Settings	Replacement Settings
ClientRegistration	`keyStore`	Replaced by `keystore`
The environment variable and system property that define the file system directory for configuration files.	`OPENIG_BASE` and `openig.base`	Replaced by `IG_INSTANCE_DIR` and `ig.instance.dir` If neither the deprecated setting nor the replacement setting are provided, configuration files are in the default directory `$HOME/.openig` (on Windows, `%appdata%\OpenIG`). If the deprecated setting and the replacement setting are both provided, the replacement setting is used.
OpenAmAccessTokenResolver	`endpoint`	Replaced by the AmService property `url`. For information, see OpenAmAccessTokenResolver in OAuth2ResourceServerFilter(5) in the *Configuration Reference*.
PolicyEnforcementFilter	`amHandler`, `openamUrl`, `realm`, and `ssoTokenHeader`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader`
	`cache` property `maxTimeout`	Replaced by `cache` property `maximumTimeToCache`
SingleSignOnFilter	`amHandler`, `openamUrl`, `realm`, and `cookieName`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader` For information, see SingleSignOnFilter(5) in the *Configuration Reference*.
TokenTransformationFilter	`amHandler`, `openamUri`, `realm`, and `ssoTokenHeader`	Replaced by the AmService properties `amHandler`, `url`, `realm`, and `ssoTokenHeader`.

Configuration Object	Deprecated Settings	Replacement Settings
		For information, see TokenTransformationFilter(5) in the *Configuration Reference*.
`OAuth2ResourceServerFilter`	cacheExpiration	Replaced by `cache` and its sub-properties `enabled`, `defaultTimeout`, and `maxTimeout`. If `cacheExpiration` is configured and `cache` is not configured, the cache is enabled and the value of `cacheExpiration` is used as `maxTimeout`. The following values for `cacheExpiration`, supported in previous releases, are not supported in this release: `zero`, `unlimited`. For more information, see OAuth2ResourceServerFilter(5) in the *Configuration Reference*.

3.3. Removed Functionality

No functionality has been removed in this release of IG.

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 release 6.1.

4.1. Key Fixes

This release of IG fixes the following important issues:

- OPENIG-2695: UI: Unable to open Freeform editor on Linux

- OPENIG-2634: UI: Uncaught error on route error

4.2. Limitations

This release of IG includes the following limitations:

Proxy WebSocket Traffic

IG cannot proxy WebSocket traffic for TLS connections, or when it is running in the Jetty application container.

For more information, see "*Proxying WebSocket Traffic*" in the *Gateway Guide*, and the `websocket` property of ClientHandler(5) in the *Configuration Reference* or ReverseProxyHandler(5) in the *Configuration Reference*.

JwtBuilderFilter to Pass Identity or Other Runtime Info Downstream

The JWT created by JwtBuilderFilter is not encrypted. Carefully consider the security of your configuration when using this filter.

For more information, see JwtBuilderFilter(5) in the *Configuration Reference* and JwtBuilderContext(5) in the *Configuration Reference*.

systemProxy Can't Be Used With Proxy Requiring Username and Password

The ClientHandler and ReverseProxyHandler property `systemProxy` can't be used with a proxy that requires a username and password. Use the handler's `proxy` property instead.

For more information, see the `agent` property of ClientHandler(5) in the *Configuration Reference* and ReverseProxyHandler(5) in the *Configuration Reference*.

Fail To Receive AM WebSocket Notifications with Jetty

When IG runs on Jetty 9.2.x or 9.4.8, WebSocket notifications are not received correctly. To work around this issue, comment out the entry `-module=websocket` in Jetty's `start.ini` file.

For more information, see the `agent` property of AmService(5) in the *Configuration Reference*.

Support for UMA Is Experimental

IG provides experimental support for building a UMA resource server, with the capability and limitations described in "*Supporting UMA Resource Servers*" in the *Gateway Guide*.

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

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 "Creating Routes Through Studio " in the *Gateway Guide*.

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, IG can check server certificates. However, mutual authentication, where IG presents its client certificate, is not supported if the client certificate is not the first certificate in the ClientHandler or ReverseProxyHandler keystore.

IG Scripts Can Access Anything in Their Environment

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

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.

`CookieFilter` **is not JwtSession compatible**

The CookieFilter heap object stores a java.net.CookieManager reference in the `session`, so that cookies are linked to the HTTP session. This behavior is not compatible with the use of a JwtSession.

SAML v2.0 Federation does not work if the user defined mapping is incorrectly set

If the user defined mapping is incorrectly set, missing SAML assertions produce an infinite loop during authentication attempts.

4.3. Known Issues

This release of IG includes the following known issues:

- OPENIG-2144: AuditService and JmsAuditEventHandler : failure on Jboss

- OPENIG-1628: Script update referenced in route, not taken into account

- OPENIG-1557: UI: Unable to deploy route when custom router is configured

- OPENIG-813: auditService : fileRotation may overwrite existing audit file

- OPENIG-659: CryptoHeaderFilter - error on handling header value with incorrect length

FORGEROCK

Chapter 5
Documentation Changes

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

- 2020-04-15: Correction in SAML routes with multiple service providers.

- 2020-04-15: Correction to the `AMCtxId` property name.

- New chapter "*Proxying WebSocket Traffic*" in the *Gateway Guide*

- New reference pages JwtBuilderFilter(5) in the *Configuration Reference* and JwtBuilderContext(5) in the *Configuration Reference*

Appendix A. Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

A.1. ForgeRock Product Release Levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

Release Level Definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated • Include changes present in previous Minor and Maintenance releases
Minor	Version: x.y[.0] (trailing 0s are optional)	• Bring minor features, and bug fixes

Release Label	Version Numbers	Characteristics
		• Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces
		• Can remove previously Deprecated functionality
		• Include changes present in previous Minor and Maintenance releases
Maintenance, Patch	Version: x.y.z[.p] The optional `.p` reflects a Patch version.	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release

A.2. ForgeRock Product Interface Stability

ForgeRock products support many protocols, APIs, GUIs, and command-line interfaces. Some of these interfaces are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines interface stability labels and uses these definitions in ForgeRock products.

Interface Stability Definitions

Stability Label	Definition
Stable	This documented interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	This documented interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release. While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.
Deprecated	This interface is deprecated and likely to be removed in a future release. For previously stable interfaces, the change was likely announced in a previous release. Deprecated interfaces will be removed from ForgeRock products.
Removed	This interface was deprecated in a previous release and has now been removed from the product.
Technology Preview	Technology previews provide access to new features that are evolving new technology that are not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to

Stability Label	Definition
	change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT. Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums. ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an "AS-IS" basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.
Internal/Undocumented	Internal and undocumented interfaces can change without notice. If you depend on one of these interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. Getting Support

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

B.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.

B.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

B.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, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.