



Release Notes

/ ForgeRock Identity Gateway 6.5

Latest update: 6.5.0

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 © 2012-2018 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. This license is available with a FAQ at: <http://scripts.sil.org/OFL>.

Table of Contents

Preface	iv
1. What's New	1
1.1. New Features	1
1.2. Product Improvements	5
1.3. Security Advisories	6
2. Before You Install	7
2.1. Downloading IG Software	7
2.2. Java Requirements	7
2.3. Web Application Containers	7
2.4. AM Java Agents	8
2.5. Features Supported With ForgeRock Access Management	8
2.6. Third-Party Software Required for Encryption	9
3. Compatibility With Other Releases	10
3.1. Important Changes to Existing Functionality	10
3.2. Deprecated Functionality	11
3.3. Removed Functionality	15
4. Fixes, Limitations, and Known Issues	17
4.1. Key Fixes	17
4.2. Limitations	17
4.3. Known Issues	19
5. Documentation Changes	20
A. Release Levels and Interface Stability	21
A.1. ForgeRock Product Release Levels	21
A.2. ForgeRock Product Interface Stability	22
B. Getting Support	24
B.1. Accessing Documentation Online	24
B.2. How to Report Problems or Provide Feedback	24
B.3. Getting Support and Contacting ForgeRock	25

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)

Chapter 1

What's New

IG 6.5 provides new features and improvements.

1.1. New Features

This release of IG includes the following new features:

Commons Secret Service

IG now leverages the ForgeRock Commons Secrets Service for the management of passwords and secrets in the following objects: AmService, ClientHandler, ClientRegistration, JwtSession, KeyManager, JwtBuilderFilter, and CapturedUserPasswordFilter.

Managing secrets with the Commons Secrets Service provides the following benefits:

- Separation from other configuration so that configuration can be moved between environments
- Storage in different secure backends, including file-based keystores, Hardware Security Modules (HSM), and Key Management Systems (KMS)
- Provision through environment variables or unencrypted JSON, for deployment simplicity or where host/OS security is considered adequate.
- Ease of rotation or revocation, regardless of the storage backend.

In this release, routes generated in Studio do not use the Commons Secrets Service. Documentation examples generated with Studio use deprecated properties.

For information about the SecretsService, see [Secrets](#) in the *Configuration Reference*. For information about new and deprecated properties, see "[Compatibility With Other Releases](#)".

Local Validation of Stateless Access-Tokens

The StatelessAccessTokenResolver is now available to validate stateless access_tokens without referring to AM. Use StatelessAccessTokenResolver with the access_token resolver in OAuth2ResourceServerFilter.

Because IG can validate stateless access_tokens locally, without referring AM, this feature provides the following benefits:

- Improved performance, by reducing the number of network hops required for validation

- Improved robustness, by validating `access_tokens` even when AM is not available

Supported with OpenAM 13.5, and AM 5 and later versions.

For more information, see "Validating Stateless Access-Tokens With the `StatelessAccessTokenResolver`" in the *Gateway Guide* and `StatelessAccessTokenResolver(5)` in the *Configuration Reference*.

Transactional Authorization

IG can now respond to the `TransactionConditionAdvice` from AM to require users to perform additional actions when trying to access a resource protected by an AM policy.

Performing the additional actions successfully grants a one-time access to the protected resource. Additional attempts to access the resource require the user to perform the additional actions again.

Supported with AM 5.5 and later versions.

For more information, see "*Hardening Authorization With Advice From AM*" in the *Gateway Guide*.

Disconnection Strategy WebSocket Notification Service

IG can now configure what happens to the session cache and policy enforcement cache when the WebSocket notification service is disconnected and then reconnected. By default, the caches are cleared on disconnect.

For information, see `onNotificationDisconnection` in `AmService(5)` in the *Configuration Reference* and `PolicyEnforcementFilter(5)` in the *Configuration Reference*.

Dynamic Scope Evaluation for OAuth2ResourceServerFilter

The `OAuth2ResourceServerFilter` can now use a script to evaluate which scopes must be provided in an OAuth 2.0 `access_token` to access a protected resource. The script evaluates each request dynamically and returns the scopes that are required for the request to access the protected resource.

Use this feature when protected resources can't be grouped within a set of static scopes, for example, when one set of URLs require one scope, and another set of URLs require another scope.

For more information, see the `scopes` section and Examples section of `OAuth2ResourceServerFilter(5)` in the *Configuration Reference*.

JWT Encryption With JwtBuilderFilter

A new property, `encryption`, has been added to the `JwtBuilderFilter` to configure JWT encryption.

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

JwtBuilderFilter Template Declared as Expression

The `template` property of `JwtBuilderFilter` can now be configured as an expression that evaluates to a map. The referenced map will be serialized as a JSON object.

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

Connection to TLS-Protected Endpoints With `TlsOptions`

A new object, `TlsOptions`, is available to configure connections to TLS-protected endpoints for the `ClientHandler`, `ReverseProxyHandler`, and for `WebSocket` notifications in `AmService`.

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

Increased Flexibility for Retrieving and Caching User Profiles From AM

The `UserProfileFilter` provides new features to retrieve and cache user profile information.

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

User Authentication From OAuth 2.0 Access Tokens With `UserProfileFilter`

The `UserProfileFilter` can now retrieve AM profile attributes for users identified by their `username`, and can be used in routes that rely on `OAuth2ResourceServerFilter` and the `/oauth2/introspect` endpoint to resolve access tokens.

The filter can use the `SsoTokenContext`, `SessionInfoContext`, or `OAuth2Context` to retrieve profile attributes.

Cache for User Profile Attributes with `UserProfileFilter`

The `UserProfileFilter` can now cache user profile attributes and reuse them without repeatedly querying AM.

In previous releases, the `UserProfileFilter` had to query AM for each request to retrieve the required user profile attributes.

New Features in `AmService`

Simplified Configuration of Objects by Using `AmService Agent`

A new property, `agent`, in `AmService` defines a Java agent to act on behalf of IG, and simplify configuration of the following filters:

- `SingleSignOnFilter`, where `agent` defines the AM service to use for authentication. Users can authenticate in the same realm as the agent, or in a different realm.
- `PolicyEnforcementFilter`, where `agent` defines the AM agent with the right to request policy decisions from AM. The policy set can be located in the same realm as the agent, or in a different realm.

- `TokenTransformationFilter`, where `agent` defines the AM agent with the right to authenticate IG as an AM REST STS client.

The `agent` property is now mandatory in `AmService` and replaces properties in the above filters. For more information, see "Removed Functionality".

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

Configuration of WebSocket Notifications by Using AmService

A new property, `notifications`, has been added to `AmService` to disable WebSocket notifications, configure the time between attempts to re-establish lost WebSocket connections, and to configure WebSocket connections to TLS-protected endpoints.

For more information, see "WebSocket Notification Service" in the *Configuration Reference*.

UserProfileFilter Configuration Moved to AmService

To simplify configuration, properties in `UserProfileFilter` have been deprecated and replaced with properties in `AmService`.

For more information, see "Deprecated Configuration Settings".

StudioProtectionFilter to Restrict Access to Studio In Development Mode

A new filter, `StudioProtectionFilter`, is available to protect the Studio endpoint when IG is running in development mode.

When IG is running in development mode, by default the Studio endpoint is open and accessible. When `StudioProtectionFilter` is defined in `admin.json`, IG uses it to filter access to the Studio endpoint.

For an example configuration, see "Restricting Access to Studio in Development Mode" in the *Gateway Guide*. For more information about `StudioProtectionFilter`, see "Provided Objects" in the *Configuration Reference*.

New Features in Studio

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

- Configure a `SplunkAuditEventHandler`.
- Upgrade HTTP connections to WebSocket protocol.
- Enable a session cache.
- Evaluate scopes dynamically for OAuth 2.0 authorization.

New Features in Freeform Studio

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

- Create new routes that contain a `SingleSignOnFilter`, a `PolicyEnforcementFilter`, and an example `AmService`. Select the objects to configure them.
- Drag and drop a `SingleSignOnFilter`, a `PolicyEnforcementFilter`, or any filter type onto the canvas. Select the filter to configure it. For other filter types, select the type, name the filter, and add the JSON configuration.
- Define multiple `AmService` objects that you can choose from for filters.
- Drag and drop a `DispatchHandler` onto the canvas, select its input node to connect it to the start element or another object, and select its output node to connect to one or more handlers. Select the connections to define the conditions for the dispatch.
- Drag any filter into or out of a chain, and drag any filter or handler around the canvas. Select it to delete it.
- Ctrl-click to select multiple objects, and maneuver or delete them at the same time.
- View unconnected filters or handlers on the canvas as part of the JSON heap.
- View the object name on the canvas.

Routes created in previous version of Freeform Studio are automatically transitioned into JSON editor routes.

1.2. Product Improvements

This release of IG includes the following improvements:

TimerDecorator Publishes Metrics to the MetricRegistry

When a `TimerDecorator` is set to `true` in a route, the metrics are now written to the Prometheus Scrape Endpoint and the ForgeRock Common REST Monitoring Endpoint.

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

Audit Logging to Standard Output

Support has been added for an audit handler to send access log messages to standard output.

For information, see `JsonStdoutAuditEventHandler(5)` in the *Configuration Reference* and "Recording Audit Events to Standard Output" in the *Gateway Guide*.

Default Configurations for Objects In AdminHttpApplication

`AdminHttpApplication` now declares default configurations for the following objects: `ClientHandler`, `ReverseProxyHandler`, `ForgeRockClientHandler`, `ScheduledThreadPoolExecutor`, and `TransactionIdOutboundFilter`.

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

Improved Security for Authentication Cookies in `CrossDomainSingleSignOnFilter` and `JwtSession`

By default, the `JwtCookieSession` cookie and `CrossDomainSingleSignOnFilter` authentication cookie and are now flagged as `HttpOnly`.

`CrossDomainSingleSignOnFilter` has additional properties to set or unset cookie flags for `HttpOnly` and `secure`. For more information, see `CrossDomainSingleSignOnFilter(5)` in the *Configuration Reference*.

WebSocket Traffic for TLS Connections

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

For information, see the `websocket` property of `ClientHandler(5)` in the *Configuration Reference* or `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-6.5.0.war](#)
- Web application for testing IG configurations, [IG-sample-application-6.5.0.jar](#)

2.2. Java Requirements

The following table lists supported Java versions:

JDK Requirements

Vendor	Versions
Oracle JDK	8
OpenJDK	8, 11

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

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

2.3. Web Application Containers

IG runs in the following web application containers:

- Apache Tomcat 8 or 8.5.x, 9
- Jetty 9
- JBoss EAP 7.1

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. AM Java Agents

IG supports several versions of Java Agents. For supported container versions and other platform requirements related to agents, see the *Java Agents Release Notes*.

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

If you install an AM policy agent in the same container as IG, use Java Agents 3.5 or later. Earlier versions might not shut down properly with the web application container.

You cannot run Java Agents 5.5.0 and IG in the same Tomcat container.

2.5. 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 <code>sessionCache</code> , using WebSocket notifications from AM. For more information, see AmService(5) in the <i>Configuration Reference</i> .	AM 5.5 when the user manually whitelists the <code>AmCtxId</code> session property, and with AM 6 and later versions (where the <code>AmCtxId</code> session property is whitelisted by default).
AM password capture and replay, as described in "Getting Login Credentials From AM" in the <i>Gateway Guide</i> .	Supported with AM 5 and later versions, and with AM 6 and later versions when the <code>AES</code> keyType is used to decrypt the password.
AM policy enforcement, as described in "Enforcing Policy Decisions From AM" in the <i>Gateway Guide</i> .	AM 5 and later versions
OpenID Connect dynamic registration and discovery, as described in "Using OpenID Connect Discovery and Dynamic Client Registration" in the <i>Gateway Guide</i> .	OpenAM 13.5, and AM 5 and later versions

Feature	Supported In AM Version
Token transformation, as described in " <i>Transforming OpenID Connect ID Tokens Into SAML Assertions</i> " in the <i>Gateway Guide</i> .	OpenAM 13.5, and AM 5 and later versions
User Managed Access 2.x, for IG 5.5, as described in " <i>Supporting UMA Resource Servers</i> " in the <i>Gateway Guide</i> .	AM 5.5 and later versions
User Managed Access 1.x, for IG 5 and earlier versions.	AM 5.1 and earlier versions
Single sign-on, as described in "About SSO Using the SingleSignOnFilter" in the <i>Gateway Guide</i> .	AM 5 and later versions
Cross-domain single sign-on, as described in "About CDSSO Using the CrossDomainSingleSignOnFilter" in the <i>Gateway Guide</i> .	AM 5.5 and later versions
Capture and storage of AM session information, as described in SessionInfoFilter(5) in the <i>Configuration Reference</i> .	AM 5 and later versions
Capture and storage of AM user profile attributes, as described in UserProfileFilter(5) in the <i>Configuration Reference</i> .	AM 5 and later
Support for transactional authorization, as described in " <i>Hardening Authorization With Advice From AM</i> " in the <i>Gateway Guide</i> .	AM 5.5 and later versions
Validation of stateless access_tokens, as described in "Validating Stateless Access-Tokens With the StatelessAccessTokenResolver" in the <i>Gateway Guide</i> .	OpenAM 13.5, and AM 5 and later versions

2.6. Third-Party Software Required for Encryption

To use RSASSA-PSS for signature encryption in the JwtBuilderFilter, install Bouncy Castle. For information, see *The Legion of the Bouncy Castle*.

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 changes:

Agent Credentials Mandatory in AmService

The `agent` property of `AmService` is now mandatory. The agent defines the credentials of an AM Java agent that acts on behalf of IG to authenticate with AM, request policy decisions from AM, and communicate WebSocket notifications from AM to IG.

This is a breaking change for all filters that use `AmService`, and for the following filters where `agent` replaces properties that are removed in this release:

- `SingleSignInFilter`, where `agent` replaces previously deprecated properties.
- `PolicyEnforcementFilter`, where `agent` replaces previously deprecated properties and the following properties: `pepUsername` and `pepPassword`.
- `TokenTransformationFilter`, where `agent` replaces previously deprecated properties and the following properties: `username` and `password`.

For more information, see "Removed Functionality".

Agent Session Logged Out When AmService Stopped

When a route containing an `AmService` is reloaded, or when an `AmService` is stopped, the agent session is logged out.

For more information, see `org.forgerock.openig.tools.am.AmService`.

Disconnection Strategy for Session Cache and PolicyEnforcementFilter Cache

When the WebSocket notification service is disconnected, by default the session cache and policy enforcement cache is cleared. In previous releases, the caches were not cleared.

For information, see `onNotificationDisconnection` in `AmService(5)` in the *Configuration Reference* and `PolicyEnforcementFilter(5)` in the *Configuration Reference*.

DS API Change for Secure LDAP Connection

DS 6.5 has updated its client API for establishing SSL connections. The `SslContextBuilder` class has been removed and related usages have been integrated into `SslOptions`.

This has an impact on existing scripts that are using IG's `LdapClient` for connecting to a secure LDAP server.

Previously working script:

```
import org.forgerock.opendj.security.SslContextBuilder;
//...
SslContextBuilder builder = new SslContextBuilder();
builder.trustManager(TrustManagers.trustAll());
SslOptions sslOptions = SslOptions.newSslOptions(builder.build())
    .enabledProtocols("TLSv1.2");
```

Usage of the new API:

```
SslOptions sslOptions = SslOptions.newSslOptions(null, TrustManagers.trustAll())
    .enabledProtocols("TLSv1.2");
```

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.

In this release, routes generated in Studio do not use the Commons Secrets Service. Documentation examples generated with Studio use deprecated properties.

This section lists deprecated functionality, as defined in "ForgeRock Product Interface Stability".

IG Route Monitoring Endpoint

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

For more information, see "Prometheus Scrape Endpoint" in the *Gateway Guide*, and "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
AmService	<code>password</code>	Replaced by <code>passwordSecretId</code> . If the deprecated and replacement properties are both provided, the replacement property takes precedence.
ClientHandler	<code>proxy</code> subproperty <code>password</code>	Replaced by <code>passwordSecretId</code> . If the deprecated and replacement properties are both provided, the replacement property takes precedence.
	<ul style="list-style-type: none"> • <code>keyManager</code> • <code>sslCipherSuites</code> • <code>sslContextAlgorithm</code> • <code>sslEnabledProtocols</code> • <code>trustManager</code> 	Replaced by the <code>TlsOptions</code> object. For more information, see <code>TlsOptions(5)</code> in the <i>Configuration Reference</i> .
	<code>websocket</code> subproperties: <ul style="list-style-type: none"> • <code>keyManager</code> • <code>sslCipherSuites</code> • <code>sslContextAlgorithm</code> • <code>sslEnabledProtocols</code> • <code>trustManager</code> 	Replaced by the <code>TlsOptions</code> object. For more information, see <code>TlsOptions(5)</code> in the <i>Configuration Reference</i> .
ReverseProxyHandler	<ul style="list-style-type: none"> • <code>keyManager</code> • <code>sslCipherSuites</code> • <code>sslContextAlgorithm</code> • <code>sslEnabledProtocols</code> 	Replaced by the <code>TlsOptions</code> object. For more information, see <code>TlsOptions(5)</code> in the <i>Configuration Reference</i> .

Configuration Object	Deprecated Settings	Replacement Settings
	<ul style="list-style-type: none"> <code>trustManager</code> <p><code>websocket</code> subproperties:</p> <ul style="list-style-type: none"> <code>keyManager</code> <code>sslCipherSuites</code> <code>sslContextAlgorithm</code> <code>sslEnabledProtocols</code> <code>trustManager</code> 	Replaced by the <code>TlsOptions</code> object. For more information, see <code>TlsOptions(5)</code> in the <i>Configuration Reference</i> .
JwtSession	<code>password</code>	Replaced by <code>passwordSecretId</code> If the deprecated and replacement properties are both provided, the replacement property takes precedence.
	Combination of <code>password</code> , <code>alias</code> , and <code>keystore</code> Combination of <code>passwordSecretId</code> , <code>alias</code> , and <code>keystore</code>	Replaced by <code>encryptionSecretId</code> If the deprecated and replacement properties are both provided, the replacement property takes precedence.
	<code>sharedSecret</code>	Replaced by <code>signatureSecretId</code> If the deprecated and replacement properties are both provided, the replacement property takes precedence.
KeyManager	<code>password</code>	Replaced by <code>passwordSecretId</code> . If the deprecated and replacement properties are both provided, the replacement property takes precedence.
KeyStore	<code>password</code>	Replaced by <code>passwordSecretId</code> . If the deprecated and replacement properties are both provided, the replacement property takes precedence.
CapturedUserPasswordFilter	<code>key</code>	Replaced by <code>keySecretId</code> . If the deprecated and replacement properties are both provided, the replacement property takes precedence.

Configuration Object	Deprecated Settings	Replacement Settings
JwtBuilderFilter	<p><code>signature</code> subproperties:</p> <ul style="list-style-type: none"> <code>keystore</code> <code>alias</code> <code>password</code> 	<p>Replaced by <code>signature</code> property <code>secretId</code>.</p> <p>If the deprecated and replacement properties are both provided, the replacement property takes precedence.</p>
Route	<code>monitor</code>	<p>Replaced by the Prometheus Scrape Endpoint and Common REST Monitoring Endpoint.</p> <p>For information, see Monitoring Endpoints(5) in the <i>Configuration Reference</i>.</p>
UserProfileFilter	<code>ssoToken</code>	Replaced by <code>username</code> in <code>UserProfileFilter</code> .
	<code>amService</code> and <code>profileAttributes</code>	Replaced <code>amService</code> and <code>profileAttributes</code> , as sub-properties of <code>userProfileService</code>
ClientRegistration	<code>keyStore</code>	Replaced by <code>keystore</code> .
	<code>clientSecret</code>	<p>Replaced by <code>clientSecretId</code>.</p> <p>If the deprecated and replacement properties are both provided, the replacement property takes precedence.</p>
The environment variable and system property that define the file system directory for configuration files.	<code>OPENIG_BASE</code> and <code>openig.base</code>	<p>Replaced by <code>IG_INSTANCE_DIR</code> and <code>ig.instance.dir</code>.</p> <p>If neither the deprecated setting nor the replacement setting are provided, configuration files are in the default directory <code>\$HOME/.openig</code> (on Windows, <code>%appdata%\OpenIG</code>).</p> <p>If the deprecated setting and the replacement setting are both provided, the replacement setting is used.</p>
OpenAmAccessTokenResolver	<code>endpoint</code>	<p>Replaced by the <code>AmService</code> property <code>url</code>.</p> <p>For information, see OpenAmAccessTokenResolver in OAuth2ResourceServerFilter(5) in the <i>Configuration Reference</i>.</p>

Configuration Object	Deprecated Settings	Replacement Settings
PolicyEnforcementFilter	cache subproperty <code>maxTimeout</code>	Replaced by <code>cache</code> property <code>maximumTimeToCache</code> .
OAuth2ResourceServerFilter	<code>cacheExpiration</code>	<p>Replaced by <code>cache</code> and its sub-properties <code>enabled</code>, <code>defaultTimeout</code>, and <code>maxTimeout</code>.</p> <p>If <code>cacheExpiration</code> is configured and <code>cache</code> is not configured, the 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>

3.3. Removed Functionality

This section lists removed functionality, as defined in "ForgeRock Product Interface Stability".

Removed Configuration Settings

Configuration Object	Removed Settings	Newer Evolving Settings
PolicyEnforcementFilter(5) in the <i>Configuration Reference</i>	Deprecated previously, removed in this release: <ul style="list-style-type: none"> <code>amHandler</code> <code>openamUrl</code> <code>realm</code> <code>ssoTokenHeader</code> 	Replaced by AmService properties: <ul style="list-style-type: none"> <code>amHandler</code> <code>url</code> <code>realm</code> <code>ssoTokenHeader</code>
	Deprecated and removed in this release: <ul style="list-style-type: none"> <code>pepUsername</code> <code>pepPassword</code> 	Replaced by AmService property: <ul style="list-style-type: none"> <code>agent</code>
SingleSignOnFilter(5) in the <i>Configuration Reference</i>	Deprecated previously, removed in this release:	Replaced by AmService properties:

Configuration Object	Removed Settings	Newer Evolving Settings
	<ul style="list-style-type: none"> • <code>amHandler</code> • <code>openamUrl</code> • <code>realm</code> • <code>ssoTokenHeader</code> 	<ul style="list-style-type: none"> • <code>amHandler</code> • <code>url</code> • <code>realm</code> • <code>ssoTokenHeader</code>
TokenTransformationFilter(5) in the <i>Configuration Reference</i>	Deprecated previously, removed in this release: <ul style="list-style-type: none"> • <code>amHandler</code> • <code>openamUrl</code> • <code>realm</code> • <code>ssoTokenHeader</code> 	Replaced by AmService properties: <ul style="list-style-type: none"> • <code>amHandler</code> • <code>url</code> • <code>realm</code> • <code>ssoTokenHeader</code>
	Deprecated and removed in this release: <ul style="list-style-type: none"> • <code>username</code> • <code>password</code> 	Replaced by AmService property: <ul style="list-style-type: none"> • <code>agent</code>

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 6.5.

4.1. Key Fixes

This release of IG fixes the following important issues:

- OPENIG-3231: OpenDJ SslContextBuilder has been removed
- OPENIG-3219: When using scan feature in logback.xml the ig.instance.dir property is lost on reload
- OPENIG-3113: Not possible to use token substitutions within a monitor decorator of a Route

4.2. Limitations

This release of IG includes the following limitations:

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.

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.

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*.

Proxy WebSocket Traffic (OPENIG-3248)

When IG is running in the Jetty application container, it cannot proxy WebSocket traffic.

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*.

Blocked ClientHandler With Asynchronous HTTP Clients (OPENIG-2417)

IG processes responses from asynchronous HTTP clients by using two thread pools of the same size:

- the first thread pool receive the response headers,
- the second thread pool completes the promise by to executing the callback and writing the response content to the stream. Reading and writing to the stream are synchronous, blocking operations

When there are a lot of clients, or when responses are big, the synchronous operation can cause routes to declare a blocked `ClientHandler`.

To recover from blocking, restart the route, or, if the route is `config.json`, restart the server. To prevent blocking, increase the number of worker threads.

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

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

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.

CookieFilter Is Not JwtSession Compatible (OPENIG-458)

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`.

Cannot Use SAML With AM Policy Agent (OPENIG-291)

When SAML is used with an AM policy agent, class cast exceptions occur.

SAML Fails With Incorrect User-Defined Mapping (OPENIG-234)

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

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.

4.3. Known Issues

This release of IG includes the following known issues:

- OPENIG-3235: Support UTF-8 encoded password values for agent's credentials
- OPENIG-3221: OpenIG is decoding special character ' while sending to the backend which is causing issues
- OPENIG-659: CryptoHeaderFilter - error on handling header value with incorrect length

Chapter 5

Documentation Changes

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

- The default configuration of IG, provided by when your configuration does not include a custom `config.json` file, is now described in the Examples section of `GatewayHttpApplication(5)` in the *Configuration Reference*.
- Information about session upgrade has moved from "*Enforcing Policy Decisions From AM*" in the *Gateway Guide* to the new chapter "*Hardening Authorization With Advice From AM*" in the *Gateway Guide*.
- A description of the `readWithCharset` function has been added to `Functions(5)` in the *Configuration Reference*.
- The description of available `access_token` resolvers has moved from the `accessTokenResolvers` property of `OAuth2ResourceServerFilter(5)` in the *Configuration Reference* to the dedicated section `Access Token Resolvers` in the *Configuration Reference*.
- The examples in "*Throttling the Rate of Requests to Protected Applications*" in the *Gateway Guide* have been changed to take the grouping policy and rate policy from fields in the `OAuth2Context`.
- Documentation for the deprecated IG Route Monitoring Endpoint is removed in this release.

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)	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• Bring minor features, and bug fixes

Release Label	Version Numbers	Characteristics
		<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
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
	<p>change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT.</p> <p>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.</p> <p>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.</p>
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.