FORGEROCK®

Release Notes
/ Java Agents 5.8.2

Latest update: 5.8.2

Copyright © 2011-2021 ForgeRock AS.

Abstract

Notes covering prerequisites, fixes, and known issues for ForgeRock® Access Management Java Agents. ForgeRock Access Management provides authentication, authorization, entitlement, and federation software.

Table of Contents

Overview

Quick Start

What's New	Prepare for Deployment	Check Compatibility
Discover new features and improvements in this version.	Learn about the requirements for running Java Agents software in production.	Review key implementation changes and compatibility with previous deployments.
Review Fixes	Check Doc Updates	Get Support
Review bug fixes, limitations, and open issues.	Track important changes to the documentation.	Find out where to get professional support and training.

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.

The ForgeRock Common REST API works across the platform to provide common ways to access web resources and collections of resources.

Chapter 1
What's New

What's New in Java Agents 5.8.2

Java Agents 5.8.2 is a maintenance release. It does not introduce new features.

What's New in Java Agents 5.8.1

Installation	
	+ *JBOSS Installer Allows Profiles in Standalone Mode*
	In previous releases, the JBoss installer requested a profile only when the deployment mode was `domain`. From this release, the JBoss installer also requests a profile when the deployment mode is `standalone`.
	For more information, see "Installing the JBoss Java Agent" in the *User Guide*.

What's New in Java Agents 5.8

Performance	
	+ *Expired session cache configuration*
	Properties `org.forgerock.agents.expired.session.cache.size` and `org.forgerock.agents.sso.expired.session.cache.ttl.minutes` were added to configure an expired session cache.
	Use the cache to reduce network traffic and load on AM. When the Agent receives a request using a token in the expired session cache, it rejects the request without needing to retrieve session information from AM.
	For more information, see Expired Session Cache Max Records in the *User Guide* and Expired Session Cache Timeout in the *User Guide*
	+ *Accept SSO tokens*

Properties `org.forgerock.agents.accept.sso.tokens.enabled` and `org.forgerock.agents.ipdp.cookie.domain.list` were added to support the use of SSO tokens when the Agent and the token issuer are in the same domain.

For more information, see Accept SSO Tokens in the *User Guide* and SSO Cookie Domain List in the *User Guide*

+ *Disable and manage 302 redirects*

Properties were added to disable and manage HTTP 302 redirects. For more information, see HTTP 302 Redirects Enabled in the *User Guide*.

+ *HTTP connection pooling*

Properties were added for HTTP connection pooling. Use connection pooling to control the number of connections made by the agent to AM. Connection pooling is off by default. For more information, see "Connection Pooling" in the *User Guide*.

+ *Load balancing cookies*

Properties were added to specify load balancing cookies on behalf of the end user, for policy, session, and other calls to AM. Use these properties to reduce the number of calls that different AM instances make to the core token service.

For more information, see Load Balancer Cookie Name in the *User Guide* and Load Balancer Cookie Enabled in the *User Guide*.

| Continuous Security | + *Agent password no longer in bootstrap properties* |
| | |

For improved security, the agent password is no longer included in the bootstrap properties.

This change makes it possible to store agent properties files in a git repository or other shared location, without compromising security.

For more information, see Changed bootstrap property files.

+ *Validation of Client IP Address*

For each authenticated request, the agent can now validate that the IP address of the request originates from the IP address used for first authentication, or that it contains only acceptable changes.

For more information, see Client IP Validation Mode in the *User Guide* and Client IP Validation Address Range in the *User Guide*

+ *Improved security of Agent password encryption*

The default encryption class used to encrypt the agent password has been changed from JCEEncryption to the more secure AESWrapEncryption.

The bootstrap property to manage this configuration, `com.iplanet.security.encryptor`, has been aliased to `org.forgerock.agents.encryptor.classname`.

For more information, see org.forgerock.agents.encryptor.classname in the *User Guide*.

Policy Client Service	

+ *Policy evaluation in user authenticated realm*

A new property has been added to allow AM to evaluate policies in the realm where the user is authenticated. Use this property for applications that dynamically set the realm for authentication.

For more information, see Perform Policy Evaluation in User Authenticated Realm in the *User Guide*.

Other	

+ *Management of timeout exceptions for WebSockets*

New bootstrap properties were added to manage timeout exceptions for WebSockets.

For more information, see org.forgerock.agents.ping.websocket.after.inactive.milliseconds in the *User Guide* and org.forgerock.agents.declare.websocket.dead.after.milliseconds in the *User Guide*.

+ *Prevent URL Verification During Instalation*

The **agentadmin** command has a new option `--forceInstall` to suppress verification of the AM URL and agent URL during installation.

Use this option when URLs cannot be contacted during installation, for example, to install Java Agents in the ForgeRock Identity Cloud.

For more information, see agentadmin(1) in the *User Guide*.

Chapter 2
Requirements

ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.

Platform Requirements

Supported Operating Systems & Web Application Containers

Operating Systems (OS)	OS Versions	Web Application Containers & Minimum Supported Versions
Amazon Linux 2, CentOS, Oracle Linux, Red Hat Enterprise Linux	7, 8	Apache Tomcat 8.5, Apache Tomcat 9.0, [a] Eclipse Jetty 9 (9.4.13 or later required for JDK 11), Eclipse Jetty 10, [a]
Ubuntu Linux	16.04 LTS, [b] 18.04 LTS, 20.04 LTS	IBM WebSphere Application Server 8.5 (8.5.5.9 or later required for Java 8), IBM WebSphere Application Server 9.0, Oracle WebLogic Server 12c (12.2.1.3 or later), Oracle WebLogic Server 14c, Red Hat JBoss Enterprise Application Platform 7.2, [a b] Red Hat JBoss Enterprise Application Platform 7.3, [a] WildFly 20, [a] WildFly 21 [a]
Microsoft Windows Server	2012 R2, [b] 2016 2019	Apache Tomcat 8.5, Apache Tomcat 9.0 [a]
IBM AIX	7	IBM WebSphere Application Server 8.5.5.9 or later required for Java 8, IBM WebSphere Application Server 9.0

[a]Supports JDK 11.
[b]Support for this platform will be discontinued in a future release.

> **Important**
>
> Java Agents use the WebSocket protocol to communicate with AM. Both the Java container and the network infrastructure must support the WebSocket protocol.

AM Requirements

- Java Agents 5.8.2 supports AM 5.5 and later versions.

- Java Agents 5.8.2 requires the WebSocket protocol to communicate with AM. Both the Java container and the network infrastructure must support the WebSocket protocol.

  Refer to your network infrastructure and Java container documentation for more information about WebSocket support.

- If you are upgrading from a version earlier than 5, Java Agents 5 introduced notable changes in the configuration. For example, they dropped support for JAAS, and require you to enable a new property if you are not using the AM UI as the login page. For more information about changes introduced in Java Agents 5, refer to the Java Agents 5 Release Notes.

Java Requirements

Java Agents run in a Java container, and requires a Java Development Kit.

ForgeRock supports customers using the following Java versions. ForgeRock recommends the most recent Java update, with the latest security fixes.

Supported Java Development Kit Versions

Vendor	Version
Oracle Java	8, 11
IBM Java (WebSphere only)	8
OpenJDK	8, 11

For information on the web container requirements for JDK 11, see "Platform Requirements".

Supported Clients

The following table summarizes supported clients and their minimum required versions:

Supported Clients

Client Platform	Native Apps [a]	Chrome 62+	Internet Explorer 11+	Edge 25+	Firefox 57+	Safari 11+	Mobile Safari
Windows 8 or later	✔	✔	✔	✔[b]	✔		
Mac OS X 10.11 or later	✔	✔			✔	✔	
Ubuntu 14.04 LTS or later	✔	✔			✔		
iOS 9 or later	✔	✔					✔
Android 6 or later	✔	✔					

[a] *Native Apps* is a placeholder to indicate the platform is not limited to browser-based technologies. An example of a native app would be something written to use our REST APIs.

[b] Windows 10 only.

Special Requests

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

FORGEROCK

Chapter 3
Incompatible Changes

Incompatible Changes in Java Agents 5.8.2

No incompatible changes were introduced in this release.

Incompatible Changes in Java Agents 5.8.1

No incompatible changes were introduced in this release.

Incompatible Changes in Java Agents 5.8

The following changes introduced in this release can impact your migration from Java Agents 5.7:

+ *Changed bootstrap property files*

> The agent password is no longer included in the bootstrap properties.
>
> The following filenames are changed as a result:
>
> - `OpenSSOAgentBootstrap.properties` changed to `AgentBootstrap.properties`
>
> - `OpenSSOAgentConfiguration.properties` changed to `AgentConfiguration.properties`
>
> The following property files are added as a result:
>
> - `AgentPassword.properties`
>
> - `AgentKey.properties`
>
> For more information, see "Property Files" in the *User Guide*.

+ *File Extension for Installer Logs*

To facilitate the review of log files in Windows environments, the installer log files now have extension `.txt`, for `install.txt` and `uninstall.txt`. This change applies to all environments. In previous releases, the extension was `.log`.

+ *Directory for CSV Monitoring and Debug*

The property aliases `org.forgerock.agents.csv.monitoring.directory` and `com.iplanet.services.debug.directory` no longer refer to the same configuration.

Chapter 4
Deprecation

No features or properties are deprecated, as defined in "*Release Levels and Interface Stability*".

Chapter 5
Removed

Removed is defined in "*Release Levels and Interface Stability*".

Removed in Java Agents 5.8.2

No features or properties were removed in this release.

Removed in Java Agents 5.8.1

No features or properties were removed in this release.

Removed in Java Agents 5.8

The following features or properties were removed from this release:

+ *org.forgerock.agents.jwt.cookie.secure.enabled*

> The property `org.forgerock.agents.jwt.cookie.secure.enabled` was removed. Use `org.forgerock.agents.secure.cookies.enabled` instead.
>
> For more information, see Transmit Cookies Securely in the *User Guide*.

+ *com.iplanet.am.naming.url*

> The property `com.iplanet.am.naming.url` was removed.

+ *com.sun.identity.agents.config.service.resolver*

> The property `com.sun.identity.agents.config.service.resolver` was removed in Java Agents 5.8 but reintroduced in Java Agents 5.8.1.

Chapter 6
Fixes

Fixes in Java Agents 5.8.2

For information about security issues fixed in this release, see "Security Advisories". No additional issues were fixed in this release.

Fixes in Java Agents 5.8.1

The following issues were fixed in this release:

- AMAGENTS-4204: JASPA: Fragments feature does not work with transaction policy

- AMAGENTS-4196: JASPA: When profile attribute is not found agent should continue authorization.

- AMAGENTS-4113: JASPA: Reintroduce the original service resolver property

- AMAGENTS-4077: JASPA: Fix Port check regression and make it work in non sso only mode.

Fixes in Java Agents 5.8

The following issues were fixed in this release:

- AMAGENTS-4035: JASPA: Break two different property paths into two separate properties.

- AMAGENTS-4007: JASPA: Update the agent for the AM changes to the "subject" claim in the OIDC JWT

- AMAGENTS-3819: J2EE agent encountering "Invalid boundCount" error

- AMAGENTS-3811: JASPA: Move the encrypted password out to a separate file, along with the key

- AMAGENTS-3807: JASPA: Investigate whether the Agent Profile password should be UTF-8 encoded

- AMAGENTS-3745: JASPA - Installer needs to behave better when installing user has insufficient permissions

- AMAGENTS-3739: JASPA: Agent should fail on startup when the installer has failed to install

- AMAGENTS-3717: JASPA - Debug log rotation minutes property is not handled correctly

- AMAGENTS-3680: JASPA: Fragment processing confuses conditional login

- AMAGENTS-3679: JASPA: Fix problem with conditional login failing to match the incoming path correctly

- AMAGENTS-3678: JASPA: Fix logout URI comparison problems

- AMAGENTS-3666: Not Enforced Favicon property does not work, if java agent listens on root URL path

- AMAGENTS-3665: Java Agent does not handle wildcard in protocol for NEU rule

- AMAGENTS-3243: JASPA: Alternative Agent Port property is not set by default in UI and agent makes a Warning message because of it

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 7
Limitations

Limitations are inherent to the design, not bugs to be fixed.

Limitations in Java Agents 5.8.2

No additional limitations were introduced in this release.

Limitations in Java Agents 5.8.1

No additional limitations were introduced in this release.

Limitations in Java Agents 5.8

The following limitations are in this release:

+ *CDSSO Domain List Restrictions for WildFly and JBoss*

Cookie support in WildFly and JBoss has been implemented so that only one cookie can be set with a certain name. This prevents setting the same cookie for multiple domains.

Configuring the CDSSO Domain List policy agent property with more than one cookie domain may result in redirection loops.

To work around this issue, perform the following steps:

1. Navigate to Realms > *Realm Name* > Applications > Agents > Java > *Agent Name* > SSO.

2. Remove all cookie domains from the CDSSO Domain List (`com.sun.identity.agents.config.cdsso.domain`) property.

3. Navigate to Realms > *Realm Name* > Applications > Agents > Java > *Agent Name* > Global.

4. Configure any required entries in the Agent Root URL for CDSSO (`sunIdentityServerDeviceKeyValue`) property.

The Java agent sets the cookie domain based on the requested resource.

+ *CDSSO Domain List Restrictions for Tomcat*

Tomcat 8.0.x introduced a new cookie processor, `org.apache.tomcat.util.http.Rfc6265CookieProcessor`, that became the default cookie processor on Tomcat 8.5.x.

Due to the new cookie processor's cookie validation checks, configuring domains with leading dots (**.**) in the CDSSO Cookie Domain List property (`com.sun.identity.agents.config.cdsso.domain`) may result in the following issues:

- Java agents returning HTTP 403 errors.

- Tomcat server logging messages similar to the following:

```
ERROR: AmFilter: Error while delegating to inbound handler: CDSSO Result Task Handler, access will
 be denied
java.lang.IllegalArgumentException: An invalid domain [.example.com] was specified for this cookie
at
 org.apache.tomcat.util.http.Rfc6265CookieProcessor.validateDomain(Rfc6265CookieProcessor.java:183)
at
 org.apache.tomcat.util.http.Rfc6265CookieProcessor.generateHeader(Rfc6265CookieProcessor.java:125)
at org.apache.catalina.connector.Response.generateCookieString(Response.java:989)
at org.apache.catalina.connector.Response.addCookie(Response.java:937)
at org.apache.catalina.connector.ResponseFacade.addCookie(ResponseFacade.java:386)
at com.sun.identity.shared.encode.CookieUtils.addCookieToResponse(CookieUtils.java:412)
...
```

To work around this issue, perform one of the following actions:

- Configure the legacy cookie processor implementation, `org.apache.tomcat.util.http.LegacyCookieProcessor`, in your Tomcat server. Refer to the documentation for your version of Tomcat for more information.

- Ensure the domains entered in the CDSSO Cookie Domain List property start with a number or a letter. For example:

  Valid configuration

  ```
  com.sun.identity.agents.config.cdsso.domain[0]=example.com
  com.sun.identity.agents.config.cdsso.domain[1]=123company.com
  ```

  Invalid configuration

  ```
  com.sun.identity.agents.config.cdsso.domain[0]=.example.com
  com.sun.identity.agents.config.cdsso.domain[1]=.mycompany.com
  ```

+ *The agentadmin Command Shows Warning Messages When Using JDK 11*

The `agentadmin` command may show warning messages similar to the following when using JDK 11:

```
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.forgerock.openam.sdk.com.google.inject.internal.cglib.core.
$ReflectUtils$1 ...
WARNING: Please consider reporting this to the maintainers of
 org.forgerock.openam.sdk.com.google.inject.internal.cglib.core.$ReflectUtils$1
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
```

You can safely ignore these messages.

Chapter 8
Known Issues

Issues are tracked at https://bugster.forgerock.org/jira/browse/AMAGENTS.

Known Issues in Java Agents 5.8.2

No additional issues were opened in this release.

Known Issues in Java Agents 5.8.1

No additional issues were opened in this release.

Known Issues in Java Agents 5.8

The following important issue remained open at the time of this release:

- AMAGENTS-3912: Avoid displaying a huge stacktrace to the user when the bootstrap properties file cannot be opened

- AMAGENTS-4113: JASPA: Reintroduce the original service resolver property

Chapter 9
Documentation

Date	Description
May 2021	Release of Java Agents 5.8.2 software.
April 2021	Release of Java Agents 5.8.1 software.
February 2021	Release of Java Agents 5.8 software. In addition to the changes described elsewhere in these notes, the following important changes were made to the documentation: **New documents** • The ForgeRock Identity Cloud Guide has been added to provide examples of how to integrate your business application and APIs with ForgeRock Identity Cloud.

Appendix A. Release Levels and Interface Stability

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

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

ForgeRock Product Stability Labels

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

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

ForgeRock Stability Label Definitions

Stability Label	Definition
Stable	This documented feature or 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 feature or 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.
Legacy	This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock. You should migrate to the newer version, however the existing functionality will remain. Legacy features or interfaces will be marked as *Deprecated* if they are scheduled to be removed from the product.

Stability Label	Definition
Deprecated	This feature or interface is deprecated and likely to be removed in a future release. For previously stable features or interfaces, the change was likely announced in a previous release. Deprecated features or interfaces will be removed from ForgeRock products.
Removed	This feature or 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 considered as new technology that is not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to 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 features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. Getting Support

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

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

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.