Release Notes

/ Java Agents 5

Latest update: 5.0.1.1

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

Abstract

Notes covering new features, fixes and known issues for ForgeRock® Access Management Java agents. ForgeRock Access Management provides open source authentication, authorization, entitlement and federation software.

Table of Contents

Preface

Read these release notes before installing Java Agents 5.

The information contained in these release notes cover prerequisites for installation, known issues and improvements to the software, changes and deprecated functionality, and other important information.

About ForgeRock Identity Platform™ Software

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 in Java Agents

Before you install or update Java agents, read these release notes.

Important

Before upgrading to Java Agents 5.x, consider the following points:

- Java Agents 5.x only support AM 5.5 and later.
- Java Agents 5.x use the WebSocket protocol to receive notifications from AM. Both the Java container and the network infrastructure must support the WebSocket protocol to receive notifications from AM.
- Java Agents 5.x's configuration is considerably different from that of earlier versions. For example, if you were using custom login pages in an earlier version, you must enable a new property for backwards-compatibility.

  Read the Release Notes to understand the impact of the changes before upgrading.

1.1. Patch Releases

Java Agents 5.0.1.1

- Java Agents 5.0.1.1 Patch Release

  ForgeRock periodically issues patch releases with important fixes to bugs. Java Agents 5.0.1.1 is the latest patch release, targeted for Java Agents 5.0.1 deployments and can be downloaded from the *ForgeRock BackStage* website. To view the list of fixes in this release, see Java Agents 5.0.1.1.

  Note

  ForgeRock patch releases are aimed as a fast-track method to provide fixes to existing bugs. These fixes improve the functionality, performance and security of your deployment. No new features have been introduced.

Java Agents 5.0.1 is available for download and can be found at the *ForgeRock BackStage* website.

1.2. New Features

Java Agents 5.0.1

Java Agents 5.0.1 is a maintenance release containing key fixes and a new feature:

- **Support for Custom Redirection Login Pages**

  Starting from 5.0.1, Java Agents introduce a custom redirection login mode that supports:

  - Environments that already have customized login pages that expect user sessions to be stored in SSO tokens instead of in OIDC JWTs, whether these are XUI login pages or not.
  - Environments configured so the users cannot access the AM servers directly.
  - Environments configured so the custom login pages are not part of AM's XUI.

  To support the custom redirection login mode, Java Agents 5.0.1 include the following properties:

  - `org.forgerock.openam.agents.config.allow.custom.login`
  - OpenAM Login URL `com.sun.identity.agents.config.login.url` (this property was removed in Java Agents 5, and it has been reinstated)
  - `org.forgerock.openam.agents.config.conditional.custom.login.url`

  For more information, see Section 1.4.10, "Redirection and Conditional Redirection" in the *User Guide*.

Java Agents 5

Java Agents 5 is a major release that introduces new features, functional enhancements and fixes.

- **Communication With AM Uses the OAuth 2.0 Authorization Framework**

  Java agents and AM exchange OpenID Connect JSON web tokens (JWTs) containing the information required to authenticate clients and authorize access to protected resources. The former method of communication, platform lower-level (PLL) calls, is no longer used.

  To ensure integrity, AM signs the JWTs with the `test` key alias by default. To change the signing key, see Section 2.2, "Configuring Access Management Servers to Communicate With Java Agents" in the *User Guide*.

Decoding JWTs into JSON objects is a CPU-intensive operation. To reduce the amount of processing required on each request, Java agents cache decoded JWTs. The following properties control the cache's behavior:

- `org.forgerock.openam.agents.config.jwt.cache.size`
- `org.forgerock.openam.agents.config.jwt.cache.ttl.minutes`

For more information, see Section 1.4.11, "Caching Capabilities" and Profile Properties in the *User Guide*.

Java Agents 5 also include a new property, JWT Cookie Name (`org.forgerock.openam.agents.config.jwt.name`), that specifies the name of the cookie that holds the JWT on the user's browser. By default, this property is set to the value of `am-auth-jwt`. For more information, see Profile Properties in the *User Guide*.

- **New Container Versions Supported**

  Java Agents 5 now support the following container versions:

  - Apache Tomcat 8.5
  - JBoss Enterprise Application Platform 7
  - Jetty 9
  - Wildfly 9 and 10.1

  The list of supported operating systems has also been updated. For more information on supported containers, see Section 2.1, "Platform Requirements".

- **Support for JDK 8**

  Java Agents 5 now support the following JDKs:

  - Oracle Java 8
  - IBM Java 8 (WebSphere only)
  - OpenJDK 8

  For more information about supported JDK versions, see Section 2.3, "Java Requirements".

- **Continuous Security**

  Because Java agents are the first point of contact between users and your business applications, they can collect inbound requests' cookie and header information which an AM server-side authorization script can then process.

For example, you may decide that only incoming requests containing the `InternalNetwork` cookie can access the intranet outside working hours.

Java agents introduce two properties related to continuous security:

- Continuous Security Cookies (`org.forgerock.openam.agents.config.continuous.security.cookies`)
- Continuous Security Headers (`org.forgerock.openam.agents.config.continuous.security.headers`)

For more information about these properties, see Continuous Security Properties in the *User Guide*.

- **New Active Session Cache Timeout Property**

  Java Agents 5 include a new property, `org.forgerock.openam.agents.config.active.session.cache.ttl.minutes`, to specify the time interval in minutes after which an active session in the Java agent's cache expires.

  For more information about this property, see Policy Client Service Properties in the *User Guide*.

1.3. Major Improvements

Java Agents 5

- **Improvements to Not-Enforced Rules**

  Not-Enforced rules now support:

  - Creating compound rules, specifying not-enforced URI and IP patterns in the same rule
  - Using netmask or IP range notation when configuring the Not-Enforced Client IP List property
  - Using regular expressions in not-enforced URI and IP rules
  - Filtering for HTTP methods in not-enforced URI and IP rules

  For more information, see Not-Enforced URI Processing Properties and Not-Enforced IP Processing Properties in the *User Guide*.

- **Improved POST Data Preservation**

  The POST data preservation feature of the Java agents has improved security. The agent now:

  - Generates a random unique identifier as the dummy endpoint from which the client recovers the POST data. This identifier is then placed into an encrypted cookie and provided to the client, which protects it from being snooped.

- Links the client session and the POST data using a one-time code. During authentication, the client is provided with a cookie containing the one-time code required to access the endpoint and recover the POST data. If the client cannot provide the code (because the cookie is missing) or the code differs from the one stored with the POST data, the Java agent denies access to the endpoint.

  Therefore, if a malicious user gets hold of the endpoint string, the agent will deny access to the endpoint to that user unless they can provide the one-time code.

- Introduces two new configuration properties to manage the cache and mitigate against DoS attacks: PDP Maximum Number of Cache Entries and PDP Maximum Cache Size.

For more information, see Section 1.4.8, "POST Data Preservation" and Post Data Preservation Properties in the *User Guide*.

- **Improved Notification System**

  To receive notifications from AM, earlier versions of the Java agent required the administrator to configure bi-directional communication through load balancers, firewalls, and proxy servers. Java Agents 5 simplify the configuration by using the WebSocket protocol to keep long-running connections open with AM.

  Listeners defined in the Agent Notification URL property (`com.sun.identity.client.notification.url`) are only relevant to the old notification system and can be removed.

  Java agents also include a new property, Web Socket Connection Interval, to configure the time interval after which the agent reopens its WebSocket connection to the AM site. This property ensures that WebSocket connections from agents are spread across the AM site.

  For more information, see Section 1.4.2, "Notification System" and Profile Properties in the *User Guide*.

- **Improved Audit Logging**

  Local and remote audit messages now adhere to the log structure common across the ForgeRock Identity Platform and support propagation of the transaction ID across the platform.

  For more information, see Section 4.2, "Configuring Audit Logging" in the *User Guide*.

- **Improvements in Cross-Domain Single Sign-On**

  Cross-domain single sign-on (CDSSO) includes the following improvements:

  - CDSSO now provides single sign-on (SSO) for AM and Java agents configured in the same DNS domain and across DNS domains.

    CDSSO is the default and only SSO mode for Java agents, which simplifies the configuration.

- AM now provides CDSSO using the OAuth 2.0 protocol and the `oauth2/authorize` endpoint. The former method of providing SSO, `CDCServlet`, is no longer used.

Due to these changes, the following properties are no longer used:

- CDSSO Servlet URL (`com.sun.identity.agents.config.cdsso.cdcservlet.url`)
- Cross Domain SSO (`com.sun.identity.agents.config.cdsso.enable`)
- CDSSO Trusted ID Provider (`com.sun.identity.agents.config.cdsso.trusted.id.provider`)

For more information and implementation details, see About Single Sign-On and Configuring Cross-Domain Single Sign-On in the *ForgeRock Access Management Authentication and Single Sign-On Guide*.

Chapter 2
Before You Install

This section covers software and hardware prerequisites for installing and running Java Agents.

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.

2.1. Platform Requirements

The following table summarizes platform support:

Table 2.1. Supported Operating Systems & Web Application Containers

Operating Systems (OS)	OS Versions	Web Application Containers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	6, 7	Apache Tomcat 7 [a], 8, 8.5 JBoss Enterprise Application Platform 6 [b], 7 Wildfly 9, 10.1 IBM WebSphere Application Server 8.5 [c] Jetty 9 Oracle WebLogic Server 12c [d]
Microsoft Windows Server	2008 R2, 2012, 2012 R2, 2016	Apache Tomcat 7 [a], 8, 8.5
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache Tomcat 7 [a], 8, 8.5 Oracle WebLogic Server 12c [d]
Ubuntu Linux	14.04 LTS, 16.04 LTS	Apache Tomcat 7 [a], 8, 8.5 JBoss Enterprise Application Platform 6 [b], 7 Wildfly 9, 10.1 IBM WebSphere Application Server 8.5 [c] Jetty 9 Oracle WebLogic Server 12c [d]
IBM AIX	6, 7	IBM WebSphere Application Server 8.5 [c]

[a]Version 7.0.79 or later is required
[b]Version 6.3.3 or later is required
[c]Version 8.5.5.9 or later is required
[d]Version 12.1.3 or later is required.

Important

Java Agents use the WebSocket protocol to receive notifications from AM. Both the Java container and the network infrastructure must support the WebSocket protocol to receive notifications from AM.

2.2. Access Management Requirements

Java Agents 5 *do not* interoperate with:

- OpenAM
- AM versions earlier than 5.5.

2.3. Java Requirements

Java agents run in a Java container, and require a Java Development Kit.

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

Table 2.2. Supported Java Development Kit Versions

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

2.4. Supported Clients

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

Table 2.3. Supported Clients

Client Platform	Native Apps[a]	Chrome 33+	Internet Explorer 9+ [b]	Edge 0.1+	Firefox 28+	Safari 6.2+	Mobile Safari
Windows 7 or later	✓	✓	✓	✓	✓		
Mac OS X 10.8 or later	✓	✓			✓	✓	

Client Platform	Native Apps[a]	Chrome 33+	Internet Explorer 9+ [b]	Edge 0.1+	Firefox 28+	Safari 6.2+	Mobile Safari
Ubuntu 12.04 LTS or later	✓	✓			✓		
iOS 7 or later	✓	✓					✓
Android 4.3 or later	✓	✓					

[a] *Native Apps* is a placeholder to indicate AM is not just a browser-based technology product. An example of a native app would be something written to use AM's REST APIs, such as the sample OAuth 2.0 Token Demo app.
[b]Internet Explorer 9 is the minimum required for end users. For the administration console, Internet Explorer 11 is required.

2.5. Special Requests

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

Chapter 3

Changes and Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

3.1. Important Changes to Existing Functionality

Java Agents 5

- **`agentapp.war` Application Required**

  Java Agents 5 require the `agentapp.war` application to be deployed alongside the agent. In previous versions, deploying the application was optional.

- **Changes to Alternative Agent Port, Hostname, and Protocol Properties**

  Configuring an alternative agent port, hostname, or protocol now requires adding an entry in the Agent Root URL for CDSSO property. Failure to do so may result in redirection loops or `redirect_uri_mismatch` errors.

- **Agent Directories Renamed**

  The following agent directories have been renamed:

  - `/j2ee_agent/tomcat_v6_agent` is now `/java_agent/tomcat_agent`
  - `/j2ee_agent/jboss_v7_agent` is now `/java_agent/jboss_agent`
  - `/j2ee_agent/jetty_v61_agent` is now `/java_agent/jetty_agent`
  - `/j2ee_agent/weblogic_v10_agent` is now `/java_agent/weblogic_agent`
  - `/j2ee_agent/websphere_v61_agent` is now `/java_agent/websphere_agent`

- **Changes to Login, Logout, and Conditional Login Properties**

  Earlier versions of the Java agent could configure a number of properties to customize the login and logout URLs that the agent uses when redirecting users. Moreover, you could configure conditional login rules to redirect incoming requests from specific domains to specific AM instances.

  These properties have changed in Java Agents 5 as follows:

- Earlier versions of the Java agent authenticated users using the UI or XUI URL (which could also contain a mention of the `CDCServlet` in CDSSO flows). Therefore, login properties configured the URL to authenticate the user to a specific realm and a specific user data store. For example:

  ```
  https://openam.example.com:443/openam/UI/Login&realm=%2Fcustomers
  https://openam.example.com:443/openam/XUI/?realm=/customers#login/
  ```

  Logout properties could be configured similarly.

  Java Agents 5 authenticate to and log out users from the `oauth2/authorize` endpoint, which is not configurable. Therefore:

  - To specify the realm or authentication module to which users should authenticate to, or log out from, add a conditional redirection rule. For example:

    ```
    example.com|https://openam.example.com/openam/oauth2/authorize?realm=customers
    ```

  - The following login and logout properties have been removed from Java Agents 5:

    - OpenAM Login URL, `com.sun.identity.agents.config.login.url`

      Note

      This property has been reinstated in Java Agents 5.0.1.

    - Login URL Prioritized, `com.sun.identity.agents.config.login.url.prioritized`
    - Login URL Probe, `com.sun.identity.agents.config.login.url.probe.enabled`
    - Login URL Probe Timeout, `com.sun.identity.agents.config.login.url.probe.timeout`
    - OpenAM Logout URL, `com.sun.identity.agents.config.logout.url`
    - Logout URL Prioritized, `com.sun.identity.agents.config.logout.url.prioritized`
    - Logout URL Probe, `com.sun.identity.agents.config.logout.url.probe.enabled`
    - Logout URL Probe Timeout, `com.sun.identity.agents.config.logout.url.probe.timeout`

- Conditional login and logout properties have changed:

  - OpenAM Conditional Logout URL, `org.forgerock.openam.agents.config.conditional.logout.url`, replaces `com.sun.identity.agents.config.conditional.logout.url`.
  - OpenAM Conditional Login URL, `org.forgerock.openam.agents.config.conditional.login.url`, replaces `com.sun.identity.agents.config.conditional.login.url`.

- Earlier versions of the Java agent allowed configuring conditional login and logout redirection to several AM instances specified in the same list to balance login and logout operation across instances.

  Java Agents 5 allow one redirection URL per rule. Configure the URL of an AM site or, alternatively, a load balancer to balance connections.

- Java Agents 5 let you configure conditional login and conditional logout redirection against any service or website in your environment.

- Java Agents 5 conditional login and conditional logout properties let you specify domains, subdomains, and paths as the incoming request URL in each rule.

For more information about conditional login and conditional logout, see Login URL Properties and Logout URL Properties in the *User Guide*.

- **Changes to the Java Agent's Startup Sequence**

  The following change has been made to the Java agent's startup sequence:

  - Earlier versions of the Java agent used the bootstrap property `com.iplanet.am.naming.url` to specify the URL of the AM instance(s) the agent connects to. This property could be used to balance agent connections between AM servers in a site.

    Java Agents 5 assembles AM's URL from properties, as follows:

    ```
    com.iplanet.am.server.protocol://com.iplanet.am.server.host:com.iplanet.am.server.port/
    com.iplanet.am.services.deploymentDescriptor
    ```

    The properties used to build AM's URL are configured during agent installation. To balance agent connections to an AM site, specify the load balancer's FQDN when you are prompted for the OpenAM server URL during installation. For example:

    ```
    ...
    ---------------------------------------------
    SUMMARY OF YOUR RESPONSES
    ---------------------------------------------
    JBoss home directory : /path/to/jboss/
    JBoss deployment mode: standalone
    Install agent as global module: true
    OpenAM server URL : http://openam.loadbalancer.com:8080/openam
    Agent URL : http://www.example.com:8080/agentapp
    Agent Profile name : JBossAgent
    Agent Profile Password file name : /tmp/pwd.txt
    ...
    ```

    The `com.iplanet.am.naming.url` property is no longer used.

  - Java agents now start up when AM is not available, denying all requests to protected and not-enforced resources until AM is available.

3.2. Deprecated Functionality

Java Agents 5

- There is no deprecated functionality in this release.

3.3. Removed Functionality

Java Agents 5

- **Removed Support for the Identity Membership Environment Condition in Policies**

  Java Agents 5 does not support policies configured with the Identity Membership(`AMIdentityMembership`) environment condition. Instead, configure the equivalent User & Group (`Identity`) subject condition. For more information, see the *ForgeRock Access Management Authorization Guide*.

- **Removed Support for Several Container Versions**

  Java Agents 5 does not support the following container versions:

  - Apache Tomcat 6
  - Jboss Application Server 7
  - IBM WebSphere Application Server 8
  - Oracle WebLogic Server 11g
  - Jetty 8

  For more information on supported containers, see Section 2.1, "Platform Requirements".

- **Removed Support for Several Operating System Versions**

  Java Agents 5 do not support the following operating system versions:

  - RedHat Enterprise Linux 5
  - CentOS 5
  - Oracle Linux 5
  - Ubuntu 12.04 LTS
  - Windows Server 2008

- **Removed Support for JDK 7 and Earlier**

Java Agents 5 require JDK 8. For more information on supported JDK version, see Section 2.3, "Java Requirements".

- **Removed Support for Configuring the Agent's Encryption Provider**

  Java Agents 5 remove support for configuring the agent's encryption provider class, which now defaults to `org.forgerock.openam.shared.security.crypto.AESWrapEncryption`. Therefore, the Encryption Provider (`com.iplanet.security.encryptor`) property is no longer supported.

- **Removed Support for the Java Authentication and Authorization Service (JAAS)**

  Defining role-based access control of web resources using Java declarative security is not supported. Therefore:

  - The `com.sun.identity.agents.config.filter.mode` property no longer supports the `J2EE_POLICY` setting.
  - The following configuration properties are no longer supported:
    - Default Privileged Attribute (`com.sun.identity.agents.config.default.privileged.attribute`)
    - Privileged Attribute Type (`com.sun.identity.agents.config.privileged.attribute.type`)
    - Privileged Attributes To Lower Case (`com.sun.identity.agents.config.privileged.attribute.tolowercase`)
    - Privileged Session Attribute (`com.sun.identity.agents.config.privileged.session.attribute`)
    - Enable Privileged Attribute Mapping (`com.sun.identity.agents.config.privileged.attribute.mapping.enable`)
    - Privileged Attribute Mapping (`com.sun.identity.agents.config.privileged.attribute.mapping`)
    - WebAuthentication Available (`com.sun.identity.agents.config.jboss.webauth.available`)

- **Removed agentadmin `--migrate` Option**

  The `--migrate` early-access option has been removed from the **agentadmin** command.

  To upgrade Java agents, see Chapter 5, "*Upgrading Java Agents*" in the *User Guide*.

- **Removed Properties**

  Java Agents 5 remove support for the following configuration properties:

  - Agent Notification URL (`com.sun.identity.client.notification.url`)
  - CDSSO Clock Skew (`com.sun.identity.agents.config.cdsso.clock.skew`)
  - CDSSO Servlet URL (`com.sun.identity.agents.config.cdsso.cdcservlet.url`)

- CDSSO Trusted ID Provider (`com.sun.identity.agents.config.cdsso.trusted.id.provider`)
- Client Polling Period (`com.iplanet.am.session.client.polling.period)`)
- `com.iplanet.am.naming.url`
- Cross Domain SSO (`com.sun.identity.agents.config.cdsso.enable`)
- Default Privileged Attribute (`com.sun.identity.agents.config.default.privileged.attribute`)
- Encryption Provider (`com.iplanet.security.encryptor`)
- Enable Privileged Attribute Mapping (`com.sun.identity.agents.config.privileged.attribute.mapping.enable`)
- Login URL Prioritized (`com.sun.identity.agents.config.login.url.prioritized`)
- Login URL Probe (`(com.sun.identity.agents.config.login.url.probe.enabled)`)
- Login URL Probe Timeout (`com.sun.identity.agents.config.login.url.probe.timeout`)
- Logout URL Prioritized (`com.sun.identity.agents.config.logout.url.prioritized`)
- Logout URL Probe (`com.sun.identity.agents.config.logout.url.probe.enabled`)
- Logout URL Probe Timeout (`com.sun.identity.agents.config.logout.url.probe.timeout`)
- OpenAM Conditional Login URL, `com.sun.identity.agents.config.conditional.login.url`, replaced by `org.forgerock.openam.agents.config.conditional.login.url`
- OpenAM Conditional Logout URL `com.sun.identity.agents.config.conditional.logout.url`, replaced by `org.forgerock.openam.agents.config.conditional.logout.url`
- OpenAM Login URL (`com.sun.identity.agents.config.login.url`)
- OpenAM Logout URL (`com.sun.identity.agents.config.logout.url`)
- Policy Client Clock Skew (`com.sun.identity.policy.client.clockSkew`
- Privileged Attribute Mapping (`com.sun.identity.agents.config.privileged.attribute.mapping`)
- Privileged Attribute Type (`com.sun.identity.agents.config.privileged.attribute.type`)
- Privileged Attributes To Lower Case (`com.sun.identity.agents.config.privileged.attribute.tolowercase`)
- Privileged Session Attribute (`com.sun.identity.agents.config.privileged.session.attribute`)
- Remote Log File Name (`com.sun.identity.agents.config.remote.logfile`)
- SSO Cache Enabled (`com.sun.identity.agents.config.amsso.cache.enable`)

- Web Service Authenticator (`com.sun.identity.agents.config.webservice.authenticator`)
- Web Service Authorization Error Content File (`com.sun.identity.agents.config.webservice.autherror.content`)
- Web Service Enable (`com.sun.identity.agents.config.webservice.enable`)
- Web Service End Points (`com.sun.identity.agents.config.webservice.endpoint`)
- Web Service Internal Error Content File (`com.sun.identity.agents.config.webservice.internalerror.content`)
- Web Service Process GET Enable (`com.sun.identity.agents.config.webservice.process.get.enable`)
- Web Service Response Processor (`com.sun.identity.agents.config.webservice.responseprocessor`)
- WebAuthentication Available (`com.sun.identity.agents.config.jboss.webauth.available`)

This is a comprehensive list of all the properties removed, some of which are mentioned in other places of these release notes.

The properties are still available when creating a new agent profile in AM 5.5 to provide backwards-compatibility with earlier versions of the Java agent.

Chapter 4

Fixes, Limitations, and Known Issues

4.1. Key Fixes

Java Agents 5.0.1.1

- AMAGENTS-1805: Log level is not hotswappable on java agents 5.0

Java Agents 5.0.1

- AMAGENTS-1626: JASPA: Realm parameter set for login url should also be passed into the goto URL
- AMAGENTS-1571: Alternative Agent Port Number not working in a LB env when sso cookie is present
- AMAGENTS-1537: Agent 5 does not have standard solution for custom login pages.
- AMAGENTS-1516: JASPA: password encryption via the admin tool throws an exception
- AMAGENTS-1482: Secure Web Sockets does not work on WildFly

Java Agents 5.0.0.2

- AMAGENTS-1422: Java Agent installer has a bug around XML parsing
- AMAGENTS-1441: Java Agent5 can not start with non-datastore module in default chain
- AMAGENTS-1453: JASPA 5 (java agent) redirection (infinite) loop in sunwCDSSOUriRedirect

Java Agents 5

The following important issues were fixed in this release:

- AMAGENTS-1247: The installer manipulates (i.e. damages) the host-manager web.xml file during install
- AMAGENTS-1146: Java agent is confused about secure cookie properties
- AMAGENTS-821: Jetty_v7 j2ee agent is not compatible with jetty 9+
- AMAGENTS-791: Tomcat installer allows install into Tomcats which don't support websockets

- AMAGENTS-783: Some valid special characters set as HTTP_HEADERs are not being encoded
- AMAGENTS-409: Cookie reset is failing on Java Agents
- AMAGENTS-374: JEE Agent 3.5.1 Install fails with WildFly 10.x and EAP 7
- AMAGENTS-364: agents.config.policy.evaluation.realm does not handle realm aliases
- AMAGENTS-170: Java agent installer to ignore Tomcat version
- AMAGENTS-104: J2EE agent installer uses an old endpoint /identity/authenticate which breaks with OpenAM 13
- AMAGENTS-83: When using a site logout page, OpenAM cookies do not get cleared when trying to logout

4.2. Limitations

- **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 Doimain 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 > J2EE > *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 > J2EE > *Agent Name* > Global.
  4. Configure any required entries in the Agent Root URL for CDSSO (`sunIdentityServerDeviceKeyValue`) property.

  The Java agent will set the cookie domain based on the requested resource.

- **CDSSO Domain List Restrictions for Apache Tomcat**

  Apache Tomcat 8.0.x introduced a new cookie processor, `org.apache.tomcat.util.http.Rfc6265CookieProcessor`, that became the default cookie processor on Apache 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.
- Apache 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 Apache Tomcat server. Refer to the documentation for your version of Apache 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
```

4.3. Known Issues

Java Agents 5

The following important known issues remained opened at the time release 5 became available:

- AMAGENTS-1093: Weblogic Java agent adds an index.jsp file to the URL after authentication when a directory is requested
- AMAGENTS-896: When using local configuration and after setting log level to message we do not get any output in debug.out

Chapter 5
Documentation Updates

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

Table 5.1. Documentation Change Log

Date	Description
2018-08-03	Release of Java Agents 5.0.1.1 patch release.
2018-05-02	Maintenance release of Java Agents 5.0.1
2018-02-16	Patch release of Java Agents 5.0.0.2
2017-12-20	Initial release of Java Agents 5

Appendix A. Getting Support

For more information or resources about AM and ForgeRock Support, see the following sections:

A.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.

A.2. Using the ForgeRock.org Site

The ForgeRock.org site has links to source code for ForgeRock open source software, as well as links to the ForgeRock forums and technical blogs.

If you are a *ForgeRock customer*, raise a support ticket instead of using the forums. ForgeRock support professionals will get in touch to help you.

A.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.