OpenAM Policy Agent 3.1.0 Release Notes

Mark Craig
Vanessa Richie

Software release date: February 20, 2013

Publication date: March 07, 2013

Copyright © 2011-2013 ForgeRock AS

Abstract

Notes covering prerequisites, fixes, known issues for OpenAM policy agents. OpenAM provides open source Authentication, Authorization, Entitlement and Federation software.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit http://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.

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, MERCHANTIBILITY, 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.

Table of Contents

1. Web Policy Agents 3.1.0 1
2. Java EE Policy Agents 3.1.0 9
3. How to Report Problems & Provide Feedback 13
4. Support 15

Chapter 1. Web Policy Agents 3.1.0

This chapter concerns OpenAM web policy agents. Web policy agents run in web servers and protect access to web pages.

1.1. New in Web Policy Agents 3.1.0

Important

OpenAM Web Policy Agents 3.1.0 is a milestone release from the main development branch of the product. This Xpress release contains selected key features and all current fixed issues. An Xpress release undergoes important functional testing but not the complete testing cycle that is done for a full Enterprise release.

Xpress releases are supported through ForgeRock subscriptions and are upgradeable to the Enterprise version, which has long term support.

The goal of an Xpress release is to enable you to start build phases earlier, with the most recent features, instead of having to wait for the Enterprise release date. Fixes to issues that are discovered in an Xpress release are delivered as patches to ForgeRock customers, and are guaranteed to be delivered in the Enterprise release that follows. Xpress releases are supported for a grace period after the Enterprise version has been released.

With the exception of these Release Notes, the official documentation for this release is still in progress, and updates are accessible at http://openam.forgerock.org/docs.html. The complete, validated documentation set will be provided for the Enterprise release.

- Web policy agents can perform URL validation during the bootstrap phase when you set the `com.forgerock.agents.ext.url.validation.disable` property (OPENAM-1270).
- Web policy agents now allow you to configure the naming of the URL validation net-connect timeout (OPENAM-1257).
- Web policy agents now support IPv6 for notenforced IP addresses (OPENAM-1256).
- A web policy agent is now available for Apache HTTPD Server 2.4 (OPENAM-1195).
- Web policy agents now let you enable and disable Cache-Control headers for unauthenticated sessions (OPENAM-1087).

- Web policy agents now let you preserve POST data when working with URI-based load balancing (OPENAM-980).
- Web policy agents now let you configure whether to do an HTTP 302 redirect after processing the LARES POST (OPENAM-936).
- Web policy agents now let you configure whether to URL encode the session cookie sent with the LARES POST using the boolean property `com.forgerock.agents.cdsso.cookie.urlencode` (OPENAM-915).
- Web policy agents can now conditionally redirect users based on the incoming request URL (OPENAM-849).
- Web policy agents now support the Expires attribute on cookies (OPENAM-815).
- Web policy agents can now mark persistent cookies as HTTPOnly, to prevent scripts and third-party programs from accessing the cookies (OPENAM-804).
- The IIS 7 web policy agents now has support for HTTP Basic authentication and password replay, thereby better supporting Microsoft OWA and SharePoint (OPENAM-773).

1.2. Before You Install OpenAM Web Policy Agents

This section covers software and hardware prerequisites for installing and running OpenAM web policy agents.

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

1.2.1. Web Agents Java Requirements

All web policy agents except Microsoft IIS web agents require Java for installation. ForgeRock recommends the most recent release of Java 6 or later to ensure you have the latest security fixes.

ForgeRock has tested this release with Oracle Java SE JDK.

1.2.2. Web Agents Browsers Tested

ForgeRock has tested this web policy agent release with the following web browsers.

- Chrome release 16 and later
- Firefox 3.6 and later

- Internet Explorer 7 and later

1.2.3. Web Server Requirements

Web policy agents support the following web servers.

- Apache HTTP Server 2.0, 2.2, 2.4
- Microsoft IIS 6, 7
- Oracle iPlanet Web Server 7.0 (also known as Sun Web Server)

  In this release, this web policy agent is not at feature parity with the other web policy agents and is lacking some fixes. In particular, this policy agent has the following known issues.

  - OPENAM-2180: Missing bootstrap file in WPA for SJSWS 7 should indicate this in error message
  - OPENAM-2178: SJSWS 7 agent debug log size parameter does not behave correctly for values below 3000
  - OPENAM-2177: SJSWS does not handle PDP cache expiration correctly
  - OPENAM-1889: Wrong password in combination with naming service failover causes internal error on OpenAM
  - OPENAM-1701: Internal exception is thrown upon login to WPA when c66encode is set to false
  - OPENAM-1523: Policy Agent fails to locate OpenAM server cookie value

  This web policy agent has been tested only on 64-bit versions of Solaris.
- Sun Proxy Server 4.0 (deprecated)

1.2.4. Web Agents Platform Requirements

Apache HTTP web policy agents have been tested on Linux 2.6 or later, and on Oracle Solaris 10 or later. Apache HTTP web policy agents require Apache Portable Runtime 1.3.x or later. You can check your installation by running **httpd -v**. On some systems, the packaged version of Apache HTTP server uses earlier versions of APR that are not compatible with the current policy web agents.

The Microsoft IIS 6 web policy agent has been tested on Windows Server 2003.

The Microsoft IIS 7 web policy agent has been tested on Windows Server 2008 R2.

Before installing web policy agents on Solaris 10, make sure you have applied the latest shared library patch for C++, at least 119963-16 on SPARC, or 119964-12 on x86.

1.2.5. Web Agents Hardware Requirements

You can deploy OpenAM web policy agents on any hardware supported for the combination of software required.

ForgeRock has tested this release on x86 and x64 based systems.

1.3. Web Policy Agent Compatibility

This section concerns OpenAM Web Policy Agents 3.1.0.

1.3.1. Major Changes to Web Policy Agent Functionality

- IIS web policy agents no longer rely on the Windows registry to determine where to find configuration settings. Instead, IIS agents determine the relative location of their configuration properties files based on the location of the web policy agent DLL, and on the Site ID set by IIS at runtime.

  The cleanest upgrade path is to uninstall the previous version of the IIS agent, and then install the new version of the IIS agent.

- Naming URL validation was introduced after release 3.0.4. The initial implementation of naming URL validation for web policy agents enabled validation by default. Naming URL validation is now fully disabled by default. You can adjust this setting by using the bootstrap configuration property, `com.forgerock.agents.ext.url.validation.disable`.

1.3.2. Deprecated Functionality

The following functionality is deprecated in OpenAM Web Policy Agents 3.1.0, and is likely to be removed in a future release.

- Web policy agent support for Sun Proxy Server is deprecated. Support for Sun Proxy Server is likely to be removed in a future release.

1.3.3. Removed Functionality

No functionality has been removed in OpenAM Web Policy Agents 3.1.0.

1.4. Web Policy Agents Fixes, Limitations, & Known Issues

OpenAM web policy agent issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM.

1.4.1. Key Fixes

The following bugs were fixed in release 3.1.0. For details, see the OpenAM issue tracker.

- OPENAM-2182: Apache PA will crash when Post Data Preservation is enabled and POST data is empty
- OPENAM-2135: IIS and SJSWS policy agents should not require Host header as per HTTP/1.0 specification
- OPENAM-2125: IIS7 policy agent might crash reading POST data
- OPENAM-1838: IIS7 policy agent might crash when HOST header is not available
- OPENAM-1673: IIS6 policy agent crash on IIS application pool restart
- OPENAM-1568: Apache Policy Agent on Windows crash inside NSS/NSPR cleanup
- OPENAM-1541: Policy Agents need to be consistent in HTTP response codes when post data preservation cache entry is expired (or not available)
- OPENAM-1523: Policy Agent fails to locate OpenAM server cookie value
- OPENAM-1510: Policy Agent may crash with remote audit log enabled
- OPENAM-1448: IIS6 policy agent returns http 415 error when used with SOAP web-services and custom headers
- OPENAM-1344: Wrong library being loaded by Apache 2.4 policy agent
- OPENAM-1339: Empty audit log message for Windows policy agents
- OPENAM-1271: webagent namingUrl validation fails if datastore auth module is not configured within auth-chain of agent realm
- OPENAM-1264: OpenAM Web Agent crashes while cleaning Agent Config
- OPENAM-1208: IIS6 policy agent stuck in a loop on a session refresh advice
- OPENAM-1190: IIS6 policy agent erroneously overwrites http headers
- OPENAM-1178: IIS6 policy agent does not set proper status code on 403/500 responses in IIS6 log
- OPENAM-1176: memory leaks in libamsdk
- OPENAM-1166: IIS6 policy agent does not set Content-Type on redirect

- OPENAM-1159: IIS7 policy agent crash on unresolvable naming service hostname
- OPENAM-1118: Policy agent on Linux core dumps on disabled or invalid notifications
- OPENAM-1099: IIS7 policy agent crash on empty LARES response
- OPENAM-1015: "Invalid pointer" in agent's cleanup_properties()
- OPENAM-1011: IIS7 agent unneeded logging fills up agent log file
- OPENAM-845: Semicolon (;) appended to HTTP_HEADER values in IIS7 agent after implementing fix for OPENAM-437
- OPENAM-693: PA should not SIGSEGV if the agent configuration is invalid
- OPENAM-690: Unprotected IIS Websites Stopped Working
- OPENAM-672: IIS crashes with WebAgent
- OPENAM-617: Invalid properties in the agent profile causes the PA to SIGSEGV

1.4.2. Limitations

OpenAM web policy agents do not currently support IPv6.

1.4.3. Known Issues

The following important known issues remained open at the time release 3.1.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-1927: Silent Installation does not work for Apache2.4/Suse11
- OPENAM-1521: Cookie Hijacking Prevention does not work properly under FireFox
- OPENAM-1520: Apache 2.2 WPA 3.0.4.5 causes Apache to hang
- OPENAM-1503: Cookies configured in OpenAM not reset after logout
- OPENAM-1472: Cookie not reset at logout
- OPENAM-889: Agent should recover if the admin session gets invalid
- OPENAM-834: logout url functionality not working as expected
- OPENAM-404: Policy agent should remove duplicate response headers

- OPENAM-329: Apache 2.2 stop responding when debug log rotation is enabled in Policy Agent
- OPENAM-308: IIS6 Policy Web Agent doesn't support multiple sites correctly

Chapter 2. Java EE Policy Agents 3.1.0

This chapter concerns OpenAM Java EE policy agents. Java EE policy agents run in web application containers and protect Java EE applications.

Important

OpenAM Java EE Policy Agents 3.1.0 is a milestone release from the main development branch of the product. This Xpress release contains selected key features and all current fixed issues. An Xpress release undergoes important functional testing but not the complete testing cycle that is done for a full Enterprise release.

Xpress releases are supported through ForgeRock subscriptions and are upgradeable to the Enterprise version, which has long term support.

The goal of an Xpress release is to enable you to start build phases earlier, with the most recent features, instead of having to wait for the Enterprise release date. Fixes to issues that are discovered in an Xpress release are delivered as patches to ForgeRock customers, and are guaranteed to be delivered in the Enterprise release that follows. Xpress releases are supported for a grace period after the Enterprise version has been released.

With the exception of these Release Notes, the official documentation for this release is still in progress, and updates are accessible at http://openam.forgerock.org/docs.html. The complete, validated documentation set will be provided for the Enterprise release.

2.1. New in JavaEE Policy Agents 3.1.0

- The Java EE agent goto URL can now be modified (OPENAM-1299).
- The Apache Tomcat policy agent now supports Tomcat 7 as well (OPENAM-1273).
- Java EE policy agents can now conditionally redirect users based on the incoming request URL (OPENAM-1265).
- The auto-submitting form in `FormLoginContent.txt` now parses as valid XML (OPENAM-674).

2.2. Before You Install OpenAM Java EE Policy Agents

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

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

2.2.1. Java EE Agents Java Requirements

Java EE policy agents run in a container using Java 6 or later. ForgeRock recommends the most recent release of Java 6 or later to ensure you have the latest security fixes.

ForgeRock has tested this release with Oracle Java SE JDK.

2.2.2. Java EE Agents Browsers Tested

ForgeRock has tested this policy agent release with the following web browsers.

- Chrome release 16 and later
- Firefox 3.6 and later
- Internet Explorer 7 and later

2.2.3. Web Application Container Requirements

Java EE policy agents support the following Java EE application containers.

- Apache Tomcat 6, 7
- GlassFish v2, v3
- IBM WebSphere Application Server 7, 8, 8.5
- JBoss Enterprise Application Platform 5
- Jetty 7
- Oracle WebLogic Server 10g or later

2.2.4. Java EE Agents Platform Requirements

Apache Tomcat Java EE policy agents have been tested on Linux 2.6 or later, and on Microsoft Windows Server 2008 R2.

GlassFish Java EE policy agents have been tested on Oracle Solaris 10 or later.

Other Java EE policy agents have been tested on Linux 2.6 or later.

Testing has focused on 64-bit operating systems.

2.2.5. Java EE Agents Hardware Requirements

You can deploy OpenAM Java EE policy agents on any hardware supported for the combination of software required.

ForgeRock has tested this release on x86 and x64 based systems.

2.3. Java EE Policy Agent Compatibility

This section concerns OpenAM Java EE Policy Agents 3.1.0.

2.3.1. Major Changes to Java EE Policy Agent Functionality

No major changes affecting compatibility have been made to the OpenAM Java EE Policy Agents in this release.

2.3.2. Deprecated Functionality

No functionality has been deprecated in this release.

2.3.3. Removed Functionality

No functionality has been removed in OpenAM Java EE Policy Agents 3.1.0.

2.4. Java EE Policy Agents Fixes, Limitations, & Known Issues

OpenAM Java EE policy agent issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM.

2.4.1. Key Fixes

The following bugs were fixed in release 3.1.0. For details, see the OpenAM issue tracker.

- OPENAM-1775: Java EE agent should not encapsulate exceptions coming out of applications
- OPENAM-1357: WebSphere Policy Agent authentication issue for syncNode script when OpenAM authentication chain updated to not use Datastore as first module.
- OPENAM-1220: Invalid date header -1 with Java agents
- OPENAM-665: Uninstallation of agent on Glassfish 3 does cleanly reset security-service element correctly.

- OPENAM-390: Hot-deployment fails for J2EE Agents
- OPENAM-276: Agent logout throws 403 after logout if cookie encoding is enabled
- OPENAM-212: RemoteUser still setted after logout when accessing not enforced URL

2.4.2. Limitations

Not all features of OpenAM Java EE policy agents work with IPv6.

Apache Tomcat can fail to shut down properly when the Java EE policy agent for Tomcat is deployed. To work around this limitation, add the following to your Tomcat configuration in the `<Server port="8005" shutdown="SHUTDOWN">` section.

```
<Listener
 className="org.forgerock.agents.tomcat.v6.TomcatLifeCycleListener" />
```

2.4.3. Known Issues

The following important known issues remained open at the time release 3.1.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-2188: J2EE agent doesn't work with WebSphere 6.1 32-bit
- OPENAM-1991: Tomcat doesn't shutdown properly with J2EE agent for the tomcat.
- OPENAM-1849: J2EE profile attribute mapper cannot handle identities with special chars in universal ID
- OPENAM-1206: J2EE agent silent install isn't silent
- OPENAM-1106: Null messages in the error log
- OPENAM-868: J2EE Agent strips off servlet context when processing request for JSF application (Apache Trinidad)
- OPENAM-605: Tomcat J2ee Agent initialization fails on Windows 2003
- OPENAM-211: J2EE agents are unable to work, if the container was started prior to OpenAM

Chapter 3. How to Report Problems & Provide Feedback

If you have questions regarding OpenAM policy agents which are not answered by the documentation, there is a mailing list which can be found at https://lists.forgerock.org/mailman/listinfo/openam where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenAM 3.1.0 policy agents, 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
  - OpenAM policy agent and version
  - Any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps

Chapter 4. Support

You can purchase OpenAM support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see http://forgerock.com/partners/find-a-partner/.