OpenAM Web Policy Agent 3.3.0 Release Notes

Mark Craig
Vanessa Richie
Mike Jang

Software release date: November 08, 2013

Publication date: November 08, 2013

Copyright © 2011-2013 ForgeRock AS

Abstract

Notes covering prerequisites, fixes, known issues for OpenAM web 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 3.3.0 1
2. How to Report Problems & Provide Feedback 9
3. Support 11

Chapter 1. Web Policy Agents 3.3.0

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 3.3.0

Important

This release contains fixes that resolve security issues within web policy agents. It is strongly recommended that you update to this release to make your deployment more secure, and to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

- All of the web policy agents have been updated to include support for Internet Protocol version 6 (IPv6) support, in addition to support for IPv4.
- Web policy agents now encrypt the value of the `com.sun.identity.agents.-config.certdb.password` property (OPENAM-2479).
- Web policy agents debug logs now show the full REST URL accessed during the bootstrap process (OPENAM-2397).
- This release adds a new web policy agent for Varnish Cache (OPENAM-1362). The Varnish Cache web policy agent does not require a Java environment to use its **agentadmin** command. The Varnish Cache policy agent also uses a directory called `vmods`. This is the location used to handle any required installation or Varnish Cache updates. The user running Varnish Cache must have access to update the `vmods` directory.
- Web policy agents can perform naming URL validation during the bootstrap phase, and can fail over from one OpenAM service to another (OPENAM-1258, OPENAM-1270). Configure these capabilities by using the following bootstrap properties.

  `com.forgerock.agents.ext.url.validation.default.url.set`
  : Indicates order of service URLs for failover

  `com.forgerock.agents.ext.url.validation.level`
  : Controls the extent of naming URL validation

  `com.forgerock.agents.ext.url.validation.ping.interval`
  : Sets seconds between validation requests against the naming URL

  `com.forgerock.agents.ext.url.validation.ping.miss.count`
  : Sets threshold of validation failures after which to fail over

`com.forgerock.agents.ext.url.validation.ping.ok.count`
: Sets threshold of validation successes after which to fail back to the first URL in the `default.url.set` list

See *Bootstrap Configuration Properties* for details.

- 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).
- Web policy agents now allow use of regular expressions in Not Enforced URLs (OPENAM-772). In addition, regular expressions are supported for logout URLs and for rejecting access to invalid URLs.
- Web policy agents can now forward injected attributes to Not Enforced URLs (OPENAM-770). Set `com.sun.identity.agents.config.notenforced.url.attributes.enable=true` in the web policy agent profile as described in *Agent Configuration Properties*.

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

ForgeRock recommends the most recent update of the supported version of Java to ensure you have the latest security fixes.

All web policy agents except those associated with Varnish Cache and Microsoft IIS require a Java 6 or 7 runtime environment for installation. ForgeRock recommends the most recent update of Java 6 or 7 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 2.2, 2.4
- Microsoft IIS 6, 7, 8
- Oracle iPlanet Web Server 7.0 (also known as Sun Web Server)
- Varnish Cache 3.0.3

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.

The Microsoft IIS 8 web policy agent has been tested on Windows Server 2012.

The Varnish Cache web policy agents have been tested on Linux 2.6 or later, and on Oracle Solaris 10 or later.

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, and also on Solaris SPARC systems.

1.3. Web Policy Agent Compatibility

This section concerns OpenAM Web Policy Agents 3.3.0.

1.3.1. Important 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.level`.

- The default policy evaluation mode for new policy agent profiles is now self rather than subtree, in order to better scale for large numbers of policy rules.

Upgrade does not change existing policy agent profile configurations, however. If you want to adopt the new default setting for existing policy agents, you must change the setting manually.

For web policy agents, set `com.sun.identity.agents.config.fetch.from.root.resource=false`.

1.3.2. Deprecated Functionality

Support for Microsoft IIS 6 is deprecated, and likely to be removed in a future release.

1.3.3. Removed Functionality

- The web policy agent bootstrap property `com.forgerock.agents.ext.url.validation.disable` introduced in release 3.1.0 has been superseded by the bootstrap property `com.forgerock.agents.ext.url.validation.level`.
- Web policy agent support for Apache HTTP Server 2.0 is no longer provided in this release.
- Web policy agent support for Oracle iPlanet Web Proxy Server (formerly Sun Java System Web Sun Proxy Server) is no longer provided in this release.

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 3.3.0. For details, see the OpenAM issue tracker.

- OPENAM-3062: WebAgents do not handle notifications - caches not being flushed
- OPENAM-2952: WPA might crash in conditional login parser module
- OPENAM-2898: WPA does not set Expires attribute in all cookie reset modules
- OPENAM-2741: Web policy agent is not clearing profile/session/response headers and cookies

- OPENAM-2706: IIS is crashed by using one level wildcard to not enforced URL list
- OPENAM-2498: Varnish PA ignores com.sun.identity.agents.config.get.client.host.name property
- OPENAM-2457: IIS7 policy agent might crash inside request header modifier
- OPENAM-2244: Web Policy Agent might crash inside its reference counted pointer implementation
- 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-834: logout url functionality not working as expected
- 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-618: Agent for multi-process servers fails if OpenAM is running in SSL mode with NSPR error -8023
- OPENAM-617: Invalid properties in the agent profile causes the PA to SIGSEGV
- OPENAM-329: Apache 2.2 stop responding when debug log rotation is enabled in Policy Agent

1.4.2. Limitations

- Web policy agents for IIS do not support Web gardens nor multi-process mode.
- If you are running an Apache Web agent on RHEL 6 (CentOS 6), and are also running SELinux in enforcing mode, Apache may fail to restart with a 'Permission denied' message, with a pointer to a file in the `/path/to/web_agents/apache2x_agent/lib` directory. SELinux expects most library files to be configured with a `lib_t` label; you can set that up with the **chcon -t lib_t /path/to/web_agents/apache2x_agent/lib/*.so** and **semanage fcontext -a -t lib_t /path/to/web_agents/apache2x_agent/lib/*.so** commands.

1.4.3. Known Issues

The following important known issues remained open at the time release 3.3.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-2974: agentadmin should allow to configure multiple instances for the same agent on the same host
- OPENAM-2969: Basic policy to allow HTTP GET fails on root resource
- OPENAM-2471: IIS/SJSWS agent enforces access to agent logout URL
- OPENAM-1927: Silent Installation does not work for Apache2.4/Suse11
- OPENAM-1889: Sun Web Server policy agent: Wrong password in combination with naming service failover causes internal error on OpenAM
- 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-889: Agent should recover if the admin session gets invalid
- OPENAM-404: Policy agent should remove duplicate response headers
- OPENAM-308: IIS6 Policy Web Agent doesn't support multiple sites correctly

Chapter 2. 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 3.3.0 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 3. 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/.