OpenAM Web Policy Agent 3.3.4 Release Notes

MarkCraig
GeneHirayama
MikeJang

,
, ,

Abstract

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

Table of Contents

Chapter 1

Web Policy Agents 3.3.4

Important

OpenAM Web Policy Agents 3.3.4 is a maintenance release that resolves a number of issues, including security issues.

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.

1.1 New in Web Policy Agents 3.3.4

The following new settings have been added to this release:

- **OPENAM-4265**. Improved IIS site support. If the agent module is enabled for a site that does not have a corresponding `Instance_{siteid}` directory, the request will not be interrupted by the agent and will continue to other IIS modules, including `.net`. For more information, see OPENAM-4265.
- **OPENAM-4888**. Introduces one new setting in the bootstrap file: `com.forgerock.agents.nss.shutdown = on | off`. Default is `on` (not set) and indicates that the agent tries to close NSS connections. For more information, see OPENAM-4888.

1.2 OpenAM Web Policy Agent Documentation

You can read the following additional product documentation for OpenAM policy agents 3.3.0 online at http://docs.forgerock.org/.

- OpenAM Web Policy Agent 3.3.0 Release Notes
- OpenAM Web Policy Agent 3.3.0 Installation Guide
- OpenAM Web Policy Agent 3.3.0 Reference

1.3 Before You Install OpenAM Web Policy Agents

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

1.3.1 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 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.

1.3.2 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

1.3.3 Web Server Requirements

Web policy agents support the following web servers.

- Apache HTTP Server 2.2, 2.4
- Microsoft IIS 7, 8
- Oracle iPlanet Web Server 7.0 (also known as Sun Web Server)

1.3.4 Web Agents Platform Requirements

Apache HTTP web policy agents run on Linux 2.6.18 or later, and on Oracle Solaris 10 or later.

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.

Before installing web policy agents on Linux, make sure the system can run **gcc** 4.4.7. `libc.so.6` must be available and it must support the GLIBC_2.3 ABI. You can check this by running the following command: **strings libc.so.6 | grep GLIBC_2**. Also, `libstdc++.so.6` must be available and it must support GLIBCXX_3.4 and CXXABI_1.3. You can check this by running the following commands: **strings libstdc++.so.6 | grep GLIBCXX_3** and **strings libstdc++.so.6 | grep CXXABI_1**.

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.

1.3.5 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.

1.3.6 Special Requests

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

1.4 Upgrading & Installing Web Policy Agents

ForgeRock recommends that you update web policy agents to this release. If you are installing OpenAM web policy agents for the first time, you can use the same installation instructions as for 3.3.0.

Procedure 1.1. To Upgrade From Web Policy Agents 3.3

1. Back up the policy agent installation and configuration directories.

Also back up the configuration if it is stored centrally in OpenAM.

2. Redirect client traffic away from the protected application.
3. Stop the web server where the policy agent is installed.
4. Remove the old policy agent as described in the *Web Policy Agent Installation Guide*.

   If the uninstallation process has changed, refer to the version of the *Web Policy Agent Installation Guide* that corresponds to your web policy agent.
5. Install the new policy agent using the existing configuration.
6. Start the web server where the policy agent is installed.

   For new features, the policy agent uses the default configuration until you make changes.
7. Validate that the policy agent is performing as expected.
8. Allow client traffic to flow to the protected application.

Procedure 1.2. To Install Web Policy Agents

If you have not yet installed and configured Web Policy Agents, then install this release instead of 3.3.0.

1. Download and unzip the policy agents.

   Find a link to the OpenAM download page from http://forgerock.com/download-stack/.
2. Follow the instructions in the *OpenAM Web Policy Agent 3.3.0 Installation Guide*.

1.5 Web Policy Agent Compatibility

This section concerns OpenAM Web Policy Agents 3.3.4.

1.5.1 Important Changes to Web Policy Agent Functionality

The following changes are new in OpenAM Web Policy Agents 3.3.4.

- OPENAM-4265 introduces improved IIS site support. If the agent module is enabled for a site that does not have a corresponding `Instance_{siteid}`

directory, the request will not be interrupted by the agent and will continue to other IIS modules, including `.net`.

This change however does not add support for multiple sites and/or multiple processes in IIS. We only support one configuration/site per agent dll (instance). Also, directories should be removed from the `web_agents` directory.

- OPENAM-4629 introduces two net settings. The first is `com.forgerock.agents.init.retry.wait`, which sets the wait time (in seconds) between retries. Default (not set) value is 0.

  The second setting is `com.forgerock.agents.init.retry.wait`, which sets the wait time (in seconds) between retries. Default (not set) value is 0.

  If `Hot-Swap Enabled = no`, then both properties have no value.

- OPENAM-4888 introduces one new setting in the bootstrap file: `com.forgerock.agents.nss.shutdown = on | off`. Default is `on` (not set) and indicates that the agent tries to close NSS connections.

The following change was listed in OpenAM Web Policy Agents 3.3.3.

- On Linux, library requirements have changed. Make sure the system can run **gcc** 4.4.7. `libc.so.6` must be available and it must support the GLIBC_2.3 ABI. You can check this by running the following command: **strings libc.so.6 | grep GLIBC_2**. Also, `libstdc++.so.6` must be available and it must support GLIBCXX_3.4 and CXXABI_1.3. You can check this by running the following commands: **strings libstdc++.so.6 | grep GLIBCXX_3** and **strings libstdc++.so.6 | grep CXXABI_1**.

The following changes were listed in OpenAM web policy agents 3.3.1 and later.

- Consistency has been improved in how OpenAM policy rules match resources. Policy rules are now interpreted more consistently in line with the documentation, and more consistently across platforms and across self and subtree modes. Before you upgrade, consider how these changes affect policy rules.

  Although the changes introduced by the improvements affect mainly edge cases, they do impact deployments relying on previous, inconsistent behaviors. The following points describe how OpenAM and policy agents behave following upgrade from OpenAM 11.0.0 and web policy agents 3.3.0 to OpenAM 11.0.1 and web policy agents 3.3.1 or later.

  - Policy agents configured to use subtree mode behave as they did prior to 3.3.0.

- If you created your policies with OpenAM 11.0.0 and web policy agents 3.3.0, then note that trailing slashes are no longer stripped from resource names (OPENAM-3509, OPENAM-3667).

  In order to match a trailing slash, your rule must end in a slash, or a slash followed by a wildcard.

- When policy agents are configured to use self mode, trailing wildcards, except after `?`, match zero or more characters.

- When policy agents are configured to use self mode, previously a trailing wildcard after a slash, `/*`, matched one or more characters, whereas it now matches zero or more. This means that a resource ending in `/` previously would not match a rule ending in `/*`, whereas it now does.

  If you already have two rules to allow access, one ending in `/` and the other in `/*`, then you have nothing to do. Only the latter rule is now required.

  If however you have only rules ending in `/*` and intend these to deny access to resources ending in `/`, then add rules ending in `/` specifically to deny access to resources ending in `/`.

- When web policy agents are configured to use self mode, trailing wildcards after `?` match *one* or more characters. This means that a resource with a trailing `?` no longer matches a rule of the form `/*?*`, whereas it would have matched with earlier versions.

  To match the behavior of previous releases, when using self mode with resources having empty query strings, add additional rules without trailing wildcards as in `/*?` before you upgrade OpenAM.

This is the only compatibility change since release 3.3.0.

The following changes were listed for OpenAM Web Policy Agents 3.3.0.

- 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`.

1.5.2 Deprecated Functionality

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

1.5.3 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 Proxy Server) is no longer provided in this release.

1.6 Web Policy Agents Fixes, Limitations, & Known Issues

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

> **Important**
>
> Starting with policy agents version 3.3.1 and OpenAM version 11.0.1, OpenAM web policy agents address backward compatibility with earlier agents. For details, make sure that you read Section 1.5.1, “Important Changes to Web Policy Agent Functionality”.

1.6.1 Key Fixes

The following bugs were fixed in release 3.3.4. For details, see the OpenAM issue tracker.

- OPENAM-889: Agent should recover if the agent session gets invalid
- OPENAM-3325: IIS7 PA might crash when logout url is not available
- OPENAM-3692: WPA build script should not depend on products.xml
- OPENAM-4166: Notification queue processor does not start in custom apache mpm configuration
- OPENAM-4265: Support for multiple app pools within a single IIS site/server instance
- OPENAM-4285: WPA local audit log file is not rotating
- OPENAM-4414: Apache Policy Agent does not complete cleanup / logout
- OPENAM-4428: IIS7 WPA post data preservation module does not return HTTP 501 error for POST with invalid Content-Type
- OPENAM-4629: Web policy agent 3.3.3 fails to connect to OpenAM when http starts first, doesn't continuously try to reconnect
- OPENAM-4851: SJSWS WPA notification processor exits with incorrect SAF exit code
- OPENAM-4888: Apache WPA might fail to recycle its worker process when any other Apache HTTPD module is using NSS/NSPR
- OPENAM-5068: WPA ignores notenforced.url.attributes.enable parameter while clearing http headers/cookies
- OPENAM-5288: WPA might fail to connect to IPv6 only host with PR_ADDRESS_NOT_AVAILABLE_ERROR error

1.6.2 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.

1.6.3 Known Issues

The following important known issues remained open at the time release 3.3.4 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-308: IIS6 Policy Web Agent doesn't support multiple sites correctly
- OPENAM-404: Policy agent should remove duplicate response headers
- OPENAM-1503: Cookies configured in OpenAM not reset after logout
- OPENAM-1520: Apache 2.2 WPA 3.0.4.5 causes Apache to hang
- OPENAM-1521: Cookie Hijacking Prevention does not work properly under FireFox
- OPENAM-1889: Sun Web Server policy agent: Wrong password in combination with naming service failover causes internal error on OpenAM
- OPENAM-1927: Silent Installation does not work for Apache2.4/Suse11
- OPENAM-2974: agentadmin should allow to configure multiple instances for the same agent on the same host
- OPENAM-3875: 'Encode URL's Special Characters' in Web Agent does not consistently encode the / charater
- OPENAM-4360: WPA does not create agent profile automatically when OpenAM is running with HTTPS

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 3.3.4 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/.