OpenAM Web Policy Agent Release Notes

Version 4

Mark Craig
Mike Jang
Chris Lee
Vanessa Richie

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

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
What's New

Before you install OpenAM Web Policy Agents or update your existing installation, read these release notes. Then update or install OpenAM Web Policy Agents.

1.1. Major New Features in 4.0.1

OpenAM Web Policy Agents 4.0.1 is a maintenance release that resolves a number of fixes and security issues. See Section 4.1.1, "Key Fixes in 4.0.1" and Section 1.3, "Security Advisories".

1.2. Major New Features in 4.0.0

OpenAM Web Policy Agents 4.0.0 is a major release that introduces new features and functional enhancements.

This release introduces the following product enhancements:

- **Multi-site Support on IIS**. Web policy agents 4 support multiple sites configured within IIS. Each site in IIS has its own web policy agent configuration. The web policy agents displays a list of the sites available in IIS during installation:

```
c:\> agentadmin.exe --i
    IIS Server Site configuration:

    Number of Sites: 2
    id: 1   name: "DEFAULT WEB SITE"
    id: 2   name: "CUSTOMERPORTAL"

    Enter IIS Server Site identification number.
    [ q or 'ctrl+c' to exit ]
```

  For more information, see Section 5.2, "Installing IIS Web Policy Agents" in the *OpenAM Web Policy Agent User's Guide*.

- **Virtual Hosts Support on Apache**. Web policy agents 4 support installing agents into multiple virtual hosts on Apache web servers. Each virtual host has its own web policy agent configuration.

- **Automated Permissions**. Folders that need to be written to by user the web server is running as can have their permissions applied automatically. Web policy agents installed into IIS set the required permissions by default. When installed into Apache answer `yes` when prompted:

```
Change ownership of created directories using
     User and Group settings in httpd.conf
     [ q or 'ctrl+c' to exit ]
     (yes/no): [no]: yes
```

- **Customizable Encryption Settings**. You can configure which encryption protocols, and which ciphers are enabled for communication between the agents and OpenAM.

  For more information, see Encryption Properties in the *OpenAM Web Policy Agent User's Guide*.

1.2.1. Improvements in Web Policy Agents 4.0.0

The following improvements and additional features were added in this release:

- OPENAM-6528: WPA4 agentadmin for IIS should set instance directory ACLs
- OPENAM-4610: WPA audit log entry should also contain client IP address
- OPENAM-3775: Windows 64bit web agent nightly build target is missing Apache policy agents
- OPENAM-1812: Policy agent should support more advanced not enforced ip/url configurations
- OPENAM-1151: Provide a configurable mechanism to to exclude weak ciphers for the client

1.3. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For more information on ForgeRock's security advisory policy, click the following link: http://www.forgerock.com/services/security-policy/

Security Advisories for the OpenAM Web Policy Agents are posted on the ForgeRock Knowledge Base.

Chapter 2
Before You Install

This section covers software and hardware prerequisites for installing and running OpenAM Web Policy 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. Web Policy Agents Platform Requirements

The following table summarizes platform support.

Table 2.1. Supported Operating Systems & Web Servers

Operating Systems (OS)	OS Versions	Web Servers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	5, 6, 7	Apache HTTP Server 2.2 Apache HTTP Server 2.4
Microsoft Windows Server	2008 R2	Microsoft IIS 7 Microsoft IIS 7.5 Apache HTTP Server 2.2 [a] Apache HTTP Server 2.4 [a]
	2012, 2012 R2	Microsoft IIS 8 Apache HTTP Server 2.2 [a] Apache HTTP Server 2.4 [a]
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache HTTP Server 2.2 Apache HTTP Server 2.4
Ubuntu Linux	12.04 LTS, 14.04 LTS	Apache HTTP Server 2.2 Apache HTTP Server 2.4
IBM AIX	6, 7	Apache HTTP Server 2.2 Apache HTTP Server 2.4

[a] The Apache HTTP Server Project does not offer binary releases for Microsoft Windows. The ForgeRock Apache HTTP Server policy agent for Windows was tested against the binaries offered by Apache Lounge.

The following table summarizes OpenSSL support for SSL and TLS connections.

Table 2.2. Supported OpenSSL Versions

Operating Systems	OpenSSL Versions
CentOS Red Hat Enterprise Linux Oracle Linux Ubuntu Linux	OpenSSL 1.0.x
Microsoft Windows Server	OpenSSL 1.0.x [a]
Oracle Solaris X86/SPARC	OpenSSL 0.9.8, OpenSSL 1.0.x
IBM AIX	OpenSSL 0.9.8, OpenSSL 1.0.x

[a] On Windows operating systems, the policy agents use the native Windows SSL libraries by default.

Note

- OpenSSL 1.0.2 is required to support TLSv1.2
- OpenSSL 1.1.x or newer is not supported

Before installing web policy agents on your platform, also make sure that the system provides the required components.

Microsoft Windows Systems

Before installing the IIS 7 web policy agent on Microsoft IIS 7 or IIS 8, make sure that the optional Application Development component of Web Server (IIS) is installed. In the Windows Server 2012 Server Manager for example, Application Development is a component of Web Server (IIS) | Web Server.

Oracle Solaris Systems

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 x64. The library is bundled on Solaris 10 update 5 and later.

2.2. 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

- All agent configuration properties are now configured in a single file, `agent.conf`.

  The `agent.conf` file contains both the bootstrap properties required to communicate with an OpenAM server, which were previously stored in `OpenSSOAgentBootstrap.properties`, and local agent configuration properties, which were previously stored in `OpenSSOAgentConfiguration.properties`.

  Tip

  The **agentadmin** tool is able to import properties from the `OpenSSOAgentConfiguration.properties` during installation to aid upgrade.

- Web policy agents no longer include independent NSS/NSPR libraries for handling SSL.

  If the OpenAM server you will be connecting to uses SSL, and the operating system does not provide native `openssl` packages, then you must install OpenSSL on the agent machine.

  For information about supported OpenSSL libraries, see Table 2.2, "Supported OpenSSL Versions".

  To download OpenSSL, see https://www.openssl.org/.

- The list of switches provided by the **agentadmin** tool has changed.

  For details, see Chapter 4, "*Installing Web Policy Agents in Apache HTTP Server*" in the *OpenAM Web Policy Agent User's Guide* and Chapter 5, "*Installing Web Policy Agents in Microsoft IIS*" in the *OpenAM Web Policy Agent User's Guide*.

- Default values for the following properties in the agent configuration file have changed:

Table 3.1. Changed Property Value Defaults

Property	Previous Default	New Default
`com.sun.identity.agents.config.debug.level`	Not Set	`error`

Property	Previous Default	New Default
com.sun.identity.agents.config.connect.timeout	0	4

- The minimum allowed value for the following properties have changed:

Table 3.2. Changed Property Value Minimums

Property	Previous Minimum	New Minimum
com.sun.identity.agents.config.debug.file.size	1048576 (1 MB)	5242880 (5 MB)
com.sun.identity.agents.config.local.log.size	1048576 (1 MB)	5242880 (5 MB)

- The `crypt_util` tool and the `certutil` binaries are no longer included with Web Policy Agents 4. The functionality these provided is now incorporated into the **agentadmin** tool.

  For more information on the functionality provided by the **agentadmin** tool, see agentadmin(1) in the *OpenAM Web Policy Agent User's Guide*.

3.2. Deprecated Functionality

No features are deprecated in this release.

3.3. Removed Functionality

- Support for Microsoft IIS 6, and Oracle iPlanet Web Server, formerly known as Sun Web Server, has been removed in this release.
- The following agent configuration properties are no longer required:
  - `com.forgerock.agents.nss.shutdown`
  - `com.sun.identity.agents.config.profilename`
  - `com.sun.identity.agents.config.forward.proxy.*`

Chapter 4

Fixes, Limitations, and Known Issues

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

4.1. Key Fixes

The following issues were fixed in release 4. For details, see the OpenAM issue tracker.

4.1.1. Key Fixes in 4.0.1

The following important issues were fixed in this release:

- OPENAM-8518: When CDSSO is enabled, POST calls can become empty in the web agent resulting in a 403
- OPENAM-8366: WPA4: Session is not terminated after agent logout in CD SSO when only cdsso iPDP cookie is presented in a browser
- OPENAM-8179: WPA4 for IIS does not handle space character in request url
- OPENAM-8136: WPA4 incorrectly sets providerId Realm value on redirect to CDCServlet
- OPENAM-8134: Agent 4 flags invalid resource for any resource that contains an asterisk
- OPENAM-8127: Agent cannot validate URL when token is found in query parameters
- OPENAM-8088: WPA4: When receiving "Session was not obtained" from OpenAM, agent should deal with it as for "Invalid Session" when the session ID can be found
- OPENAM-8065: WPA4 agentadmin installer fails in send_session_request when notifications are disabled in OpenAM
- OPENAM-8039: IIS WPA4 can not read userid attribute out of policy response if com.sun.identity.agents.config.userid.param.type=LDAP
- OPENAM-7957: WPA4 Solaris agent can crash in CDSSO module during notenforced url processing
- OPENAM-7952: Fetch Attributes for Not Enforced URLs can lead to unwanted authentication request

- OPENAM-7946: WPA4 ignores override-url configuration parameters in not enforced url evaluation module
- OPENAM-7922: WPA4 httpd crashes in agent ssl handling due to memory access violation
- OPENAM-7858: WPA4 Apache agent used together with mod_rewrite is failing on URL containing a space character
- OPENAM-7775: WPA4 defaults to 300 second cookie max-age value when running in CDSSO mode
- OPENAM-7774: WPA4 erroneously sets the same data for both response and request Cookie headers
- OPENAM-7680: WPA4 Windows agent should be able to use OpenSSL libraries from its installation lib folder only
- OPENAM-7646: WPA4 extended url validator module is too noisy in debug log
- OPENAM-7578: Web Policy Agent - HTTP POST requires a valid Content-Type header value
- OPENAM-7473: WPA4 logger on windows is missing log messages
- OPENAM-7452: WPA4 agent might crash in configuration validation phase (silent install)
- AMAGENTS-1: WPA4 reads in only a limited set of session service attributes

4.1.2. Key Fixes in 4.0.0

The following important issues were fixed in this release:

- OPENAM-6356: agent_init() am_web_init failed error if multiple Apache instances are started as different users
- OPENAM-5829: Some Norwegian characters are not correctly encoded when the "Encode URL's Special Characters" is enable
- OPENAM-5068: WPA ignores notenforced.url.attributes.enable parameter while clearing http headers/cookies
- OPENAM-4428: IIS7 WPA post data preservation module does not return HTTP 501 error for POST with invalid Content-Type
- OPENAM-4414: Apache Policy Agent does not complete cleanup / logout
- OPENAM-4391: WPA does not remove consecutive forward slashes from request URI resulting in invalid policy evaluations
- OPENAM-4390: WPA might fail to sort (reorder) query parameters resulting in invalid policy evaluation
- OPENAM-4199: Web policy agent might fail to parse URL when there is no port value specified

- OPENAM-2781: WPA does not support more than one agent instance running on the same host

4.2. Limitations

- 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 `/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 /web_agents/apache2x_agent/lib/*.so** and **semanage fcontext -a -t lib_t /web_agents/apache2x_agent/lib/*.so** commands.
- If you are using the `mod_cgid` module in your Apache installation the web policy agents cannot support the `restart` or `graceful` Apache options.

  A workaround is to use a `stop` option followed by a `start` option for restarting the Apache HTTP Server. (OPENAM-7325)

4.3. Known Issues

The following important known issues remained open at the time release 4 became available. For details and information on other issues, see the OpenAM issue tracker.

4.3.1. Known Issues in 4.0.1

The following important issues remained open when OpenAM Web Policy Agents 4.0.1 became available:

- OPENAM-8656: It is possible to select not existing siteID on installation although installation fails - with no helpful message
- OPENAM-8624: It is possible to silently install agent for site which already has one agent configured on Win2012
- OPENAM-8439: WPA property com.sun.identity.agents.config.local.audit.logfile does not work from AM console
- OPENAM-7352: WPA 4: com.sun.identity.agents.config.encode.url.special.chars.enable is not used into wpa4
- OPENAM-7291: Fix performance problems caused by cache eviction algorithm
- OPENAM-7089: WPA4: It is not possible to create an agent profile during installation WPA

The following issues remained open when OpenAM Web Policy Agents 4.0.1 became available, but are fixed in the next release:

- OPENAM-8428: WPA records audit logs to a local file although "Audit Log Location" is set to REMOTE
- OPENAM-1769: agentadmin should return exit codes other then 0
- AMAGENTS-42: Percent encoded hash (#) (%23) is handled incorrectly during policy evaluation
- AMAGENTS-32: Audit logging in WPA 4.0.0 includes requests for not enforced URLs
- AMAGENTS-27: WPA4 needs a configurable option to bypass POST data inspection
- AMAGENTS-26: Attributes Processing does not map multiple values

4.3.2. Known Issues in 4.0.0

The following important issues remained open when OpenAM Web Policy Agents 4.0.0 became available:

- OPENAM-7352: WPA 4: com.sun.identity.agents.config.encode.url.special.chars.enable is not used into wpa4
- OPENAM-7291: Fix performance problems caused by cache eviction algorithm
- OPENAM-7089: WPA4: It is not possible to create an agent profile during installation WPA
- OPENAM-6857: WPA 4: Agent version in debug log does not contain an agent platform or build machine

Chapter 5
Documentation Updates

The following table tracks changes to the documentation set following the release of OpenAM Web Policy Agents 4:

Table 5.1. Documentation Change Log

Date	Description
2016-04-14	Maintenance release of OpenAM Web Policy Agents 4.0.1. • Removed documentation on checking for existence of `libc.so.6`, which is no longer required in this version. • Removed documentation that OpenSSL libraries be copied to the `%SystemRoot%/System32/` folder, which is no longer required in this version.
2015-02-25	Initial release of OpenAM Web Policy Agents 4.0.0.

Chapter 6
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/.

Chapter 7

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 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