



Web Policy Agent Release Notes

Version 4.1

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

Copyright © 2011-2016 ForgeRock AS

Abstract

Notes covering prerequisites, fixes, known issues for ForgeRock® Access Management web policy agents. ForgeRock Access Management provides 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 <https://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.

ForgeRock® and ForgeRock Identity Platform™ are trademarks of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. 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, MERCHANTABILITY, 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.

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <http://fontawesome.io>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>.

Table of Contents

Preface	iv
1. What's New in Web Policy Agents	1
1.1. New Features in 4.1	1
1.2. New Features in 4	2
2. Before You Install	4
2.1. Web Policy Agents Platform Requirements	4
2.2. Special Requests	6
3. Changes and Deprecated Functionality	7
3.1. Important Changes to Web Policy Agent Functionality	7
3.2. Deprecated Functionality	8
3.3. Removed Functionality	8
4. Web Policy Agents Fixes, Limitations, and Known Issues	9
4.1. Key Fixes	9
4.2. Limitations	13
4.3. Known Issues	14
5. Documentation Updates	16
A. Getting Support	17
A.1. Accessing Documentation Online	17
A.2. Using the ForgeRock.org Site	17
A.3. Getting Support and Contacting ForgeRock	18

Preface

Read these release notes before you install the Web Policy Agent.

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)

Chapter 1

What's New in Web Policy Agents

Before you install AM web policy agents or update your existing web policy agent installation, read these release notes.

1.1. New Features in 4.1

- **New NGINX Plus Policy Agent**

Web Policy Agents 4.1 include a new policy agent that supports NGINX Plus web servers. For more information, see Section 2.1, "Web Policy Agents Platform Requirements" and Chapter 5, *Installing Web Policy Agents in NGINX Plus* in the *Web Policy Agent Guide*.

The NGINX Plus policy agent supports regular expressions to improve conditional login URL redirection. For more information, see the Regular Expression Conditional Login URL property on Section 8.1.4, "Configuring Access Management Services Properties" in the *Web Policy Agent Guide*.

- **Improved Logging and Caching**

Web Policy Agents 4.1 have re-engineered logging and agent policy caching functionality for improved stability and performance.

- **New JSON-Formatted Response Properties**

Additional properties for controlling JSON-formatted responses are available in Web Policy Agents 4.1.

For more information, see *JSON-Formatted Response Properties* in the *Web Policy Agent Guide*.

- **New Garbage Collector Statistics Log**

Garbage collector statistics for all policy agent instances in the container are written into the new `web_agents/type/log/agent.log` file.

For more information, see Section 8.1.8, "Configuring Web Policy Agent Environment Variables" in the *Web Policy Agent Guide*.

- **32-bit and 64-bit Web Policy Agent Package for IIS**

New in Web Policy Agent 4.1 for IIS, there is only one downloadable package that supports both 32-bit and 64-bit IIS application pools.

- **Added Support for Windows built-in Secure Channel API**

Web policy agents installed on Windows operating systems now use the built-in Secure Channel API for SSL/TLS communications with AM by default.

For more information, see [Encryption Properties](#) in the *Web Policy Agent Guide*.

- **Relative URL Support in Access Denied Property**

You can now specify a relative path in the `com.sun.identity.agents.config.access.denied.url` property.

For more information, see [General Properties](#) in the *Web Policy Agent Guide*.

- **The agentadmin Command Now Returns Status Codes on Failure**

If running the **agentadmin** command in a script, you can now check the return value to determine if the command succeeded.

For more information, see `agentadmin(1)` in the *Web Policy Agent Guide*.

- **Added Support for PKCS#12/PFX Client Certificate Files**

On Windows operating systems you can now specify a PKCS#12/PFX client certificate file in the `com.forgerock.agents.config.cert.file` property.

For more information, see [Encryption Properties](#) in the *Web Policy Agent Guide*.

1.2. New Features in 4

- **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 4.2, "Installing IIS Web Policy Agents"](#) in the *Web Policy Agent 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 AM.

For more information, see [Encryption Properties](#) in the *Web Policy Agent Guide*.

Chapter 2

Before You Install

This chapter covers software and hardware prerequisites for installing and running web policy agent software.

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 Versions	Web Servers & Versions
CentOS	5, 6, 7	Apache HTTP Server 2.2, 2.4
Red Hat Enterprise Linux	6, 7	NGINX Plus R12
Oracle Linux		
Microsoft Windows Server	2008 R2	Microsoft IIS 7.5 Apache HTTP Server 2.2, 2.4 ^a
	2012, 2012 R2	Microsoft IIS 8 Apache HTTP Server 2.2, 2.4 ^a
Oracle Solaris x64	10, 11	Apache HTTP Server 2.2, 2.4
Oracle Solaris SPARC		
Ubuntu Linux	12.04 LTS, 14.04 LTS	Apache HTTP Server 2.2, 2.4
	14.04 LTS, 16.04 LTS	NGINX Plus R12
IBM AIX	6, 7	Apache HTTP Server 2.2, 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	OpenSSL 1.0.x

Operating Systems	OpenSSL Versions
Red Hat Enterprise Linux Oracle Linux Ubuntu Linux	
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 meets the following requirements:

Linux Systems

- 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**.
- Web Policy Agents on Linux systems require a minimum of 135 megabytes of free disk space at all times. If the amount of free space drops below this threshold, a warning similar to the following appears in the **agent.log** file:

```
[Fri Nov 11 10:02:10.138732 2016] [amagent:error] [pid 4350:tid 140545949357888] amagent_init()
status: no space left on device
[Fri Nov 11 10:02:10.138981 2016] [:emerg] [pid 4350:tid 140545949357888] AH00020: Configuration
Failed, exiting
am_log_init() free disk space on the system is only 116703232 bytes, required 134900080 bytes
```

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.
- Web Policy Agents on Windows systems require a minimum of 1.07 gigabytes of free disk space at all times. If the amount of free space drops below this threshold, a warning similar to the following appears in the **agent.log** file:

```
2016-11-10 10:12:10.291 +0000 ERROR [10716:9348] am_shm_create(): free disk space on the system is
only 528949248 bytes, required 1073627136 bytes
```

```
2016-11-10 10:12:10.291 +0000 ERROR [10716:9348] get_memory_segment(): shared memory error: blocks
```

After making more disk space available, you will need to restart the web policy agent.

Failure to free up disk space and restart the web policy agent may result in errors similar to the following:

```
2016-11-10 10:19:43.610 +0000 ERROR [3764:9348] OpenAMHttpModule(): agent init for site 1 failed  
(error: -31)
```

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 Web Policy Agent Functionality

- **UTF-8 strings in headers are now MIME-encoded**

Web Policy Agents now base64-encode UTF-8 strings in headers, then wrap the string as described in RFC 2047:

```
encoded-word = "=?" charset "?" encoding "?" encoded-text "=?"
```

For example, given a UTF-8 username, such as `dēmø`, Web Policy Agents will:

1. Encode the string in base64 format: `yZfDq8mxw7g=`.
2. Wrap the base64-encoded string as per RFC 2047: `=?UTF-8?B?yZfDq8mxw7g=?=`.

- **Unencoded URLs are now passed to AM**

Web Policy Agents no longer encode paths before passing them to AM for policy evaluation. AM will receive the path with the same formatting as provided by the user agent.

For example, given a URL containing UTF-8 characters, such as `http://www.example.com/bon/café`, Web Policy Agents will pass this exact string to AM.

AM performs its own URL encoding, so to match the example above the policy would need to be configured with the following as a resource: `http://www.example.com/bon/caféC3%A9`

You may need to add additional resource specifiers to handle the raw URL strings that are now passed on from Web Policy Agents 4.1 and newer.

- **Re-Implemented Properties for Forward Proxy Configuration**

Properties for configuring a forward proxy for communication from the web policy agent to AM have been re-implemented. They were previously removed in Web Policy Agent 4.0.0.

For information on the properties, see *Forward Proxy Custom Properties in the Web Policy Agent Guide*.

- **New Swap Size Requirements on Solaris 11 x86**

Web Policy Agent 4.1 requires that the amount of swap size on Solaris 11 x86 is configured to be at least as large as the amount of available RAM.

- **32-bit and 64-bit Application Pools Support on IIS**

Web Policy Agent 4.1 now supports 32-bit and 64-bit application pools on the same IIS environment.

3.2. Deprecated Functionality

No features are deprecated in this release.

3.3. Removed Functionality

- The following agent configuration properties are no longer required:
 - `com.forgerock.agents.nss.shutdown`
 - `com.sun.identity.agents.config.profilename`

Chapter 4

Web Policy Agents Fixes, Limitations, and Known Issues

4.1. Key Fixes

4.1.1. Key Fixes in 4.1

- **AMAGENTS-269:** For remote audit logging need to be done additional configuration in OpenAM
- **AMAGENTS-262:** Update cookie reset properties to reflect new behaviour of AMAGENTS-247
- **AMAGENTS-181:** Memory leak in case of network connection failure
- **AMAGENTS-256:** Could not find a way to use a client certificate file with IIS
- **OPENAM-1769:** agentadmin should return exit codes other than 0
- **AMAGENTS-125:** "agentadmin.exe --d" command not working
- **AMAGENTS-223:** redirect loop if 'com.sun.identity.agents.config.access.denied.url' is set to absolute URL
- **OPENAM-8486:** WPA interactive installator can't correctly read provided Apache configuration path
- **OPENAM-8681:** RFE: Support com.sun.identity.agents.config.forward.proxy.* in WPA 4
- **AMAGENTS-32:** Audit logging in WPA 4.0.0 includes requests for not enforced URLs
- **AMAGENTS-47:** Agent truncates filtered HTTP POST body
- **AMAGENTS-95:** Improve Agent error handling of AM responses after OPENAM-8910
- **AMAGENTS-103:** Agent4 does not work well with mod_autoindex generated pages
- **AMAGENTS-105:** IIS Agent Crash at read of log variable after destruction by another thread at application pool recycle
- **AMAGENTS-119:** Windows Apache Agent crashes under load when constantly recycled
- **AMAGENTS-121:** Web Agent not updating headers when AM Session Attributes are changed

- **AMAGENTS-130:** IIS agent can crash in `get_request_url` method
- **AMAGENTS-132:** WPA is not able to recover from XML parser error
- **AMAGENTS-135:** WPA4 running on Schannel might not read complete HTTP response body
- **AMAGENTS-140:** WPA is not using `agents.config.polling.interval` configuration property
- **AMAGENTS-147:** Agentadmin stops in OpenAM server validation phase
- **AMAGENTS-164:** Agent with remote audit logger enabled and a little more than 4K messages agent will crash
- **AMAGENTS-173:** WPA4 on AIX does not work with a new logger
- **AMAGENTS-176:** WPA4/3.x does not support `policy.evaluation.application` config property
- **AMAGENTS-177:** WebAgent 4 not enforced URL cannot take path with 'exception'
- **AMAGENTS-186:** first agent process should delete and recreate shared memory files
- **AMAGENTS-207:** Accessing the agent logout URL without session will cause a redirect
- **AMAGENTS-208:** Agent returns HTTP 500 internal error on logout page if `com.sun.identity.agents.config.logout.url` map is empty
- **AMAGENTS-209:** Notification does not end up removing session from cache if first apache bucket contains less than 6 bytes
- **AMAGENTS-221:** Location response header not set when `'com.sun.identity.agents.config.access.denied.url'` is used
- **AMAGENTS-229:** protocol/port/host override don't work with Post Data Preservation
- **AMAGENTS-257:** IIS Agent crash in `remove_from_freelist`
- **AMAGENTS-52:** WPA on Windows should be able to use Schannel for SSL/TLS communication
- **AMAGENTS-118:** Delayed or missing log file entries possible in certain situations
- **AMAGENTS-19:** IIS agent should support mixed 32 and 64 bit application pools
- **AMAGENTS-266:** Agent recycle shutdown of shared memory occurs before all workers have finished
- **AMAGENTS-264:** Deadly embrace in log buffer handling with IIS recycling
- **AMAGENTS-248:** Agent might crash with misleading error when server is running out of disk space
- **AMAGENTS-123:** CDSSO session token cleared when hitting denied URL

- **AMAGENTS-214:** agent.log is set to debug level and it is not possible to change it
- **AMAGENTS-193:** Web Policy agent overrides Apache access control directives, Need to be documented
- **AMAGENTS-27:** WPA4 needs a configurable option to bypass POST data inspection
- **AMAGENTS-252:** WPA crashes on Solaris 11 if the swap size is not the same as the amount of RAM
- **OPENAM-8261:** Improve documentation of indexed / mapped configuration attributes
- **OPENAM-3888:** Possibility to disable redirect behaviour of the Policy Agents
- **OPENAM-8904:** OpenAM did not follow RFC 2616 and RFC 2047
- **AMAGENTS-249:** IIS Agent crash in purge of expired items or waiting for live readers when cache is shutting down in another thread
- **AMAGENTS-172:** WPA4 does not handle oversized log messages properly
- **AMAGENTS-169:** RFE: Don't depend on Apache's 'pathinfo'
- **AMAGENTS-93:** RFE: file permissions and/or ownership of log files should be configurable
- **AMAGENTS-42:** Percent encoded hash (#) (%23) is handled incorrectly during policy evaluation
- **AMAGENTS-26:** Attributes Processing does not map multiple values
- **OPENAM-8428:** WPA records audit logs to a local file although "Audit Log Location" is set to REMOTE
- **AMAGENTS-24:** Non-enforced URL validation should be lazy
- **OPENAM-8328:** WPA can't recognize custom access-denied page when there is GOTO parameter
- **AMAGENTS-70:** WPA4 Fetch attributes for Not enforced URL not entirely working
- **AMAGENTS-68:** invalid cookie causes 403 instead of redirect to login page
- **AMAGENTS-246:** Performance drop when targeting two agents on single IIS
- **AMAGENTS-225:** Under load remote audit logging produces many content length exceeded messages per batch
- **AMAGENTS-228:** With Remote audit Logging message size should be in sync with OpenAM default acceptable value 16K
- **AMAGENTS-227:** With Remote Audit logging, logging depends on time but not on buffer size which limits performance

- **AMAGENTS-231:** Agent does not log banner message on startup
- **AMAGENTS-222:** agent.conf has the wrong agent version
- **AMAGENTS-216:** Agent is crashing on Windows with more than one worker in application pool
- **AMAGENTS-211:** redirect location is not logged in case of access denied
- **AMAGENTS-144:** Apache http server 2.2 crashes on Linux systems hosted on VirtualBox
- **AMAGENTS-192:** New shared memory deletion code should handle fresh install
- **AMAGENTS-129:** Policy agent crash caused by invalid user_offset in cache file
- **AMAGENTS-185:** Possibility of hanging in ssl handshake when recycling
- **AMAGENTS-174:** WPA4 agentadmin can not complete OpenAM server validation phase
- **OPENAM-8429:** WPA audit log is not rotated when it reaches the size limit
- **AMAGENTS-133:** WPA on Windows should use Schannel as default for its SSL/TLS communication
- **AMAGENTS-122:** Agent Hangs during httpd restart on linux
- **OPENAM-8947:** Web form submitted by a POST request is truncated by the Web Policy agent
- **OPENAM-8624:** It is possible to silently install agent for site which already has one agent configured on Win2012
- **OPENAM-8656:** It is possible to select not existing siteID on installation although installation fails - with no helpful message
- **AMAGENTS-59:** Apache_v24_Linux_64bit_4.0.0 fails to install on Suse 12 SP1
- **OPENAM-8487:** Parameter --changeOwner doesn't work in WPA silent installation

4.1.2. Key Fixes in 4

New Features and Improvements

- **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

Bug Fixes

- **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

4.2.1. Limitations in 4.1

- The NGINX Plus policy agent does not support the ignore path info properties:
 - `com.sun.identity.agents.config.ignore.path.info`
 - `com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list`

4.2.2. Limitations in 4

- 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

4.3.1. Known Issues in 4.1

- **OPENAM-2396:** Agents should set 'amlbcookie' when running in CDSSO mode
- **AMAGENTS-509:** 1 CPU used per w3wp process caught in loop in read_retry
- **AMAGENTS-431:** Not Enforced URLs Are Being Protected by Policy Agent 4.x
- **AMAGENTS-382:** Apache 's Error Document does not work on any directories except for document root
- **AMAGENTS-380:** Installer fails with permissions error 0xb7 on IIS
- **AMAGENTS-357:** Installation of IIS Agent with an application pool identity type of SpecificUser results in ACL update status: error
- **AMAGENTS-349:** GET method can change into HEAD due to use of ap_method_name_of
- **AMAGENTS-322:** FastCGI module results in post data missing after processing with agent
- **AMAGENTS-317:** agentadmin --v can report 0.0 memory if there is no access to unistd.h on AIX
- **AMAGENTS-315:** Agent fails to start with insufficient shared memory
- **AMAGENTS-310:** Agents4 add well known port to goto URL when it did not exist in the original URL
- **AMAGENTS-292:** SIGBUS due to alignment issues in hashes on SPARC
- **AMAGENTS-290:** Login redirect loop in CDSSO enabled webagent
- **AMAGENTS-285:** Agent logging LOG_ALLOW or LOG_DENY does not work
- **AMAGENTS-272:** Bug in agent's net_client send/recv handling. It uses builtin/hardcoded AM_NET_POOL_TIMEOUT value of 4 sec
- **AMAGENTS-268:** 'agentadmin --v' does not show OS architecture
- **AMAGENTS-267:** not enforced IP processing broken
- **AMAGENTS-263:** Performance degradation when audit shared memory resizes

- **AMAGENTS-258:** If the Web agent Installation take more than 4 sec , it will throw "error validating OpenAM agent configuration"
- **AMAGENTS-254:** Apache's ErrorDocument does not work with Agents 4.x
- **AMAGENTS-215:** FQDN checking should be turned off by default - Web agent local file
- **AMAGENTS-178:** Invert Not Enforced does not work if Not Enforced URLs list is empty
- **AMAGENTS-46:** 4.x WPA not enforced pattern matching not consistent with 3.x

4.3.2. Known Issues in 4

- **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 AM Web Policy Agent 4.1:

Table 5.1. Documentation Change Log

Date	Description
2016-09-20	Reorganization of web policy agent documentation
2016-12-02	4.1.0 Release
2017-05-19	Web Policy Agents 4.1 documentation refresh, which includes the following updates: • NGINX Plus policy agent documentation added. For more information, see Chapter 5, <i>"Installing Web Policy Agents in NGINX Plus"</i> in the <i>Web Policy Agent Guide</i>. • Updated the procedure to create an agent profile. For more information, see Section 2.3, <i>"Creating Agent Profiles"</i> in the <i>Web Policy Agent Guide</i> • Added a procedure to upgrade web policy agents. For more information, see Chapter 6, <i>"Upgrading Web Policy Agents"</i> in the <i>Web Policy Agent Guide</i>. • Updated the list of known issues for the release. For more information, see Section 4.3.1, <i>"Known Issues in 4.1"</i>.
???	Web Policy Agents 4.1 documentation refresh, which includes the following updates: • Clarified support for OpenSSL. For more information, see Table 2.2, <i>"Supported OpenSSL Versions"</i>. • Improved documentation on the <code>org.forgerock.agents.config.keepalive.disable</code> property. For more information, see <i>Miscellaneous Custom Properties</i> in the <i>Web Policy Agent Guide</i>. • Clarified support for Apache HTTP Server for Windows. For more information, see Table 2.1, <i>"Supported Operating Systems & Web Servers"</i>. • Improved documentation for the Conditional Login URL feature. For more information, see <i>Login URL Properties</i> in the <i>Web Policy Agent Guide</i>. • Improved documentation on the <code>org.forgerock.agents.config.tls</code> property. For more information, see <i>Bootstrap Properties</i> in the <i>Web Policy Agent Guide</i>.

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, classes 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.