FORGEROCK®

Web Agents Release Notes

/ Version 4.2

Latest update: 4.2.1.2

Copyright © 2011-2019 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.

Table of Contents

Preface

Read these release notes before you install the Web Agents.

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™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

FORGEROCK

Chapter 1
What's New

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

1.1. Patch Bundle Releases

ForgeRock patch bundle releases contain a collection of fixes that have been grouped together and released as part of our commitment to support our customers. For general information on ForgeRock's maintenance and patch releases, see Maintenance and Patch Availability Policy.

Web Agents 4.2.1.2

- Web Agents 4.2.1.2 is the latest patch bundle release targeted for Web Agents 4.2.1.1[1] and 4.2.1.0 deployments and can be downloaded from the *ForgeRock Backstage* website.

  This release fixes a security issue. For more information, see "Security Advisories".

1.2. New Features

Web Agents 4.2.1.2

- No new features were introduced in this release.

Web Agents 4.2.1.1

- No new features were introduced in this release.

Web Agents 4.2.1.0

- No new features were introduced in this release.

---

[1]Web Agents 4.2.1.1 was not officially released but was issued for a client.

Web Agents 4.2

- Agents 4.2 now supports IBM HTTP server v7 and v9 on IBM AIX. Apache v22 and v24 are no longer supported on IBM AIX, but may be available upon request from Support. For more information on the supported platforms, see "Supported Operating Systems & Web Servers".

1.3. Major Improvements

Web Agents 4.2.1.2

- There are no major improvements in this release.

Web Agents 4.2.1.1

- There are no major improvements in this release.

Web Agents 4.2.1.0

- There are no major improvements in this release.

Web Agents 4.2

- **Improved Cache Performance**

  For Ajax-based applications that use key-value pairs in its URLs, there may be similar URLs that differ by key-value pair in the cache; thus, causing extra time searching through the cache. For example, the following two URLs differ by the `param2=value4|5` key-value pair in the cache:

  ```
  https://www.example.com/p1/p2?param1=value1&param2=value4&param3=value3
  https://www.example.com/p1/p2?param1=value1&param2=value5&param3=value3
  ```

  Web Agents 4.2 supports the ability for administrators to select common key-value pairs to ignore. Once the list of ignored parameters is processed, the remaining parameters are sorted alphabetically by the key. This process produces less entries in the web agent policy cache and, therefore, improves the look-up speed of cached policy evaluation.

- **Support for Load Balancers That do not Support Session Stickiness**

  Web Agents 4.2 includes a new environment variable, `AM_AGENT_REST_LOGIN`, to allow the agent to authenticate to AM servers configured behind a load balancer, which does not support session stickiness.

- **Improved Performance through Pattern-Based Policy Enforcement Rule**

Web Agents 4.2 implements a limited regular-expression-based parameter to match a specific pattern during policy evaluation. Once a policy has been selected, the results are cached for the session for the polling interval.

The regular expression-based parameter ensures that the agent's cache does not become cluttered with URL paths that are only used once per session.

- **Message Level Debug Improvements**

Web Agents 4.2 now supports improvements in message level debug logging labels. Now, `All` is the same as `Message` and provides the same output to better match AM's debug message levels. Also, the `Info`, `Message`, and `All` debug levels include additional diagnostic timing information.

For more information, see General Properties in the *Web Policy Agent Guide*.

- **Additional Improvements from Agents 4.1.0 Patches**

Web Agents 4.2 includes changes made in previous patch releases for Agents 4.1.0. To view these improvements and fixes, see Readme for Web Agents 4.1.0-40 patch in the *ForgeRock Knowledge Base*.

1.4. 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 details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base*.

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 Agents Platform Requirements

The following table summarizes platform support.

Supported Operating Systems & Web Servers

Operating Systems	OS Versions	Web Servers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	5[a]	Apache HTTP Server 2.2[b], 2.4
	6, 7	Apache HTTP Server 2.2[b], 2.4 NGINX Plus R12
Microsoft Windows Server	2008 R2	Microsoft IIS 7.5 Apache HTTP Server 2.2[b], 2.4[c]
	2012, 2012 R2	Microsoft IIS 8, 8.5 Apache HTTP Server 2.2[b], 2.4[c]
	2016	Microsoft IIS 10 Apache HTTP Server 2.2[b], 2.4[c]
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache HTTP Server 2.2[b], 2.4
Ubuntu Linux	14.04 LTS	Apache HTTP Server 2.2[b], 2.4 NGINX Plus R12
	16.04 LTS	NGINX Plus R12
IBM AIX	6.1, 7.1	IBM HTTP Server v7[d], v9[e]

[a]Centos 5 is deprecated in Agents 4.2.

[b]Apache 2.2 is deprecated in Agents 4.2. Apache 2.2 is limited to OpenSSL 1.0.x.

[c] 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.

[d]IBM HTTP server v7 is limited to OpenSSL 1.0.x. Apache 2.2 systems are limited to OpenSSL 1.0.x, IHSv7 is just one case.

[e]Apache HTTP Server v2.2 and v2.4 are available upon request. Contact Support for the patch.

The following table summarizes OpenSSL support for SSL and TLS connections. Make sure you are aware of the OpenSSL requirements for new installations if you are still on OpenSSL 0.9.8:

Supported OpenSSL Versions

Operating Systems	OpenSSL Versions
CentOS Red Hat Enterprise Linux Oracle Linux Ubuntu Linux	OpenSSL 1.0.x, OpenSSL 1.1.0, OpenSSL 1.1.1
Microsoft Windows Server	OpenSSL 1.0.x [a]
Oracle Solaris X86/SPARC	OpenSSL 0.9.8, OpenSSL 1.0.x, OpenSSL 1.1.0, OpenSSL 1.1.1
IBM AIX	OpenSSL 0.9.8, OpenSSL 1.0.x, OpenSSL 1.1.0, OpenSSL 1.1.1

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

Note

- OpenSSL 1.1.0, OpenSSL 1.1.1 and TLS v1.3 are supported for Web Agents 4.2.

- OpenSSL 1.0.1 and 1.0.2 is required to support TLSv1.2.

- OpenSSL 1.1.1 is required to support TLSv1.3.

- Windows Secure Channel does not support TLS v1.3 yet. If Windows Secure Channel is mandatory for your deployment, you can use OpenSSL.

Before installing web policy agents on your platform, also make sure that the system meets the following requirements:

Linux Systems

- Web 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 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 Agents Functionality

Web Agents 4.2.1.2

• There are no important changes to functionality in this release.

Web Agents 4.2.1.1

• There are no important changes to functionality in this release.

Web Agents 4.2.1.0

• **Property** `org.forgerock.agents.config.cdsso.deny.cleanup.disable` **Reintroduced**

Web Policy Agent 4.2.1.0 reintroduces the `org.forgerock.agents.config.cdsso.deny.cleanup.disable` property to control whether the policy agent should delete SSO cookies after receiving an HTTP 403 forbidden status.

By default, `org.forgerock.agents.config.cdsso.deny.cleanup.disable` = `false`, which specifies that the policy agent deletes the cookie after receiving an HTTP 403 forbidden status.

Note that while deleting the cookie may prevent possible CDSSO redirect loops when an unexpected 403 error occurs; the cookie deletion may cause a performance hit as additional authentication calls to AM could occur if other CDSSO nodes need the session cookie.

Depending on your environment, you may want to set this property to `true`, so that the agent does *not* delete the SSO cookie.

• **New Property** `org.forgerock.agents.config.cdsso.advice.cleanup.disable` **Introduced**

Web Policy Agent 4.2.1.0 introduces a new property, `org.forgerock.agents.config.cdsso.deny.cleanup.disable`.

When set to `true`, the policy agent will *not* reset the session cookie on an authentication redirect when a policy advice is present.

By default, `org.forgerock.agents.config.cdsso.advice.cleanup.disable` = `false`, which resets the session cookie in all configured domains for every authentication redirect when a policy advice is present.

Web Agents 4.2

• **New Agents Profiles on AM 6.x are not Compatible with Agent 4.x by Default**

New agent profiles created on AM 6.x are not compatible with Web Agents 4.x by default, causing the agent to return HTTP 403 error messages. To work around this issue, set the `com.sun.identity` `.agents.config.login.url` and `com.sun.identity.agents.config.logout.url` properties in the agent profile, otherwise the agent will return persistent 403 errors.

• **Addition of a New Environment Variable: `AM_LOG_ONE`**

Web Agents 4.2 now provides an environment variable, `AM_LOG_ONE`, to enable direct logging for an agent instance to mitigate against any performance impact when the debug logging is enabled. This variable is used for single agent instances only.

For more information, see Web Policy Agent Environment Properties in the *Web Policy Agent Guide*.

• **Incoming request URL is Shown in the `ampostpreserve` query parameter in CDSSO mode**

The `org.forgerock.agents.config.cdsso.original.url.redirect.param` custom property is still available but it is redundant in Agents 4.2.

For more information, see Miscellaneous Custom Properties in the *Web Policy Agent Guide*.

• **Support for TLSv1.3 and OpenSSL 1.1.1**

Web Agents 4.2 now supports TLSv1.3, which requires OpenSSL 1.1.1 or later.

For a list of supported protocols, see "Supported OpenSSL Versions".

3.2. Deprecated Functionality

Web Agents 4.2.1.2

• There are no deprecated features in this release.

Web Agents 4.2.1.1

• There are no deprecated features in this release.

Web Agents 4.2.1.0

• There are no deprecated features in this release.

Web Agents 4.2

Deprecated functionality are features that ForgeRock plans to remove support in a future Agents release version:

• Apache 2.2 support is deprecated in Agents 4.2.

• Centos 5 support is deprecated in Agents 4.2.

3.3. Removed Functionality

Web Agents 4.2.1.2

• There are no removed features in this release.

Web Agents 4.2.1.1

• There are no removed features in this release.

Web Agents 4.2.1.0

• There are no removed features in this release.

Web Agents 4.2

• There are no removed features in this release.

Chapter 4

Web Agents Fixes, Limitations, and Known Issues

4.1. Key Fixes

Web Agents 4.2.1.2

• A security fix was made in this release. For more information, see "Security Advisories".

Web Agents 4.2.1.1

• AMAGENTS-2547: WPA needs to handle GET request from cdcservlet

• AMAGENTS-2605: WPA write_bio_to_socket error 32

Web Agents 4.2.1.0

• AMAGENTS-2113: CDSSO PDP redirect fails when in front of CDN that adds X-Forwarded-Proto

• AMAGENTS-2175: Erroneous size data in log messages on 32bit SPARC Solaris 10 WebAgent

• AMAGENTS-2224: WPA4 crash on Windows when using OpenSSL

• AMAGENTS-2368: Agent logout url would logout SP but not IdP

• AMAGENTS-2434: Site ID set as amlbcookie causes issues when quickly validating sessions

• AMAGENTS-2441: Segmentation fault after cookie name change and debug=message

Web Agents 4.2

• AMAGENTS-323: With 4.1.0 we create more than 11 shared memory segments causing AIX32 bit to crash / fail to start

• AMAGENTS-364: agents.config.policy.evaluation.realm does not handle realm aliases

• AMAGENTS-504: default ports an not handled as expected, e.g. NotificationURL

• AMAGENTS-845: Attribute value set by session.attribute.mapping is not available

- AMAGENTS-924: 3rd party WPA 4.x http parser does not correctly handle http 1.0 / 1.1 mode switching

- AMAGENTS-1030: Nginx Web agent add Authorization header and send request along.

- AMAGENTS-1246: Improve cache performance by allowing agent to remove named parameters from urls

- AMAGENTS-1339: agentadmin --g crash on 4.1.0-27

- AMAGENTS-1391: Accelerate performance by allowing agent to cache and enforce a pattern-based agent policy enforcement rule

- AMAGENTS-1551: WPA agentadmin --g option is changing empty xml element value

- AMAGENTS-1588: agentadmin for varnish requires glibc 2.14

- AMAGENTS-1646: WPA4 for Varnish is crashing in VRB_Iterate

- AMAGENTS-1677: WPA for Varnish does not require workaround for the limited stack space anymore

- AMAGENTS-1711: Setting Message level debug on the agent results in WARN level debug.

- AMAGENTS-1738: Agent4 on AIX fails to decode session token

- AMAGENTS-1757: Missing com.sun.identity.agents.config.fqdn.default remote configuration property can crash the agent

- AMAGENTS-1759: WPA4 for IIS post data preservation + cdsso returns 404 error

- AMAGENTS-1771: WPA4 invalid JSON response with a valid session

- AMAGENTS-1781: WPA4 for IIS post data preservation + cdsso to redirect page returns 404 error

- AMAGENTS-1801: Agent does not log any OpenSSL library validation errors

- AMAGENTS-1808: Varnish agent crash in VRTPRIV_dynamic_kill

- AMAGENTS-1821: Agent4 corrupts audit log entries

- AMAGENTS-1834: Agent4 is missing com.forgerock.agents.cdsso.cookie.urlencode configuration property handler available in agent3

- AMAGENTS-1835: Adjust retry numbering to be consistent

- AMAGENTS-1857: Agent4 POST data handler results in sporadic HTTP 200 status codes

- AMAGENTS-1875: Agent4 crash in base64 encode method

- AMAGENTS-1902: Agent4 for Apache server on Windows is crashing on worker process restart

- AMAGENTS-1976: BACKPORT AMAGENTS-1348: Add option of fast direct logger

- AMAGENTS-1977: Add openssl 1.1.1 library detection for AIX web agent

- AMAGENTS-1991: Deadlock in agent4 for Apache server on Windows with remote audit enabled

4.2. Limitations

Web Agents 4.2.1.2

- There are no known limitations other than those listed in Web Agents 4.2.

Web Agents 4.2.1.1

- There are no known limitations other than those listed in Web Agents 4.2.

Web Agents 4.2.1.0

- There are no known limitations other than those listed in Web Agents 4.2.

Web Agents 4.2

The following limitations and workarounds apply to Web Agents 4.2.x:

- **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`

- **Apache HTTP Server Authentication Functionality Not Supported**

  The web agent replaces authentication functionality provided by Apache, for example, the `mod_auth_*` modules. Integration with built-in Apache httpd authentication directives, such as `AuthName`, `FilesMatch`, and `Require` is not supported.

4.3. Known Issues

Web Agents 4.2.1.2

- There are no known issues in this release.

Web Agents 4.2.1.1

- There are no known issues in this release.

Web Agents 4.2.1.0

- AMAGENTS-2440: Policy evaluation with non-ASCII character fails on Nginx

Web Agents 4.2

- AMAGENTS-377: URL with query parameters is not recognised as agent logout url

- AMAGENTS-456: URL Comparison Case Sensitivity Check does not work for policies

- AMAGENTS-554: sso-only mode does not work for specific URLs

- AMAGENTS-703: cache usage is much smaller than expected

- AMAGENTS-773: Agent Authenticator profile can't evaluate policies in sub-realm

- AMAGENTS-798: Session upgrade and custom goto parameter automated tests fail when using autodeploy for c-agent tests

- AMAGENTS-925: WPA 4 uses faulty WSAPoll feature on windows. This creates intermittent socket errors.

- AMAGENTS-1125: Session properties with tab is lost or replaced by space on Agent

- AMAGENTS-1206: com.sun.identity.agents.config.load.balancer.enable does not work from Central Profile

- AMAGENTS-1420: Nginx binaries currently fail with latest opensource Nginx

FORGEROCK

Chapter 5
Documentation Updates

The following table tracks changes to the documentation set following the release of AM Web Agents 4.2:

Documentation Change Log

Date	Description
2019-11-08	Release of Web Agents 4.2.1.2.
2019-02-08	Release of Web Agents 4.2.1.0.
	The following documentation updates were made:
	• Web Agents 4.2.x does not support OpenSSL 1.1.x for Windows Server. This has been corrected in the release notes. For more information, see "Before You Install" in the *Web Policy Agent Guide*.
	• Web Agents 4.2.1.0 introduces a new property: `org.forgerock.agents` `.config.cdsso.advice.cleanup.disable` property. For more information, see Miscellaneous Custom Properties in the *Web Policy Agent Guide*.
	• Added a tip about policy agent installation into nginx. For more information, see "To Install the Web Policy Agent into NGINX Plus" in the *Web Policy Agent Guide*.
2018-10-26	Release of Web Agents 4.2.
	The following documentation updates were made:
	• Updated cookie reset properties section to reflect that you can specify a default cookie domain. For more information, see Cookie Reset Properties in the *Web Policy Agent Guide*.
	• Updated the section on installing web policy agents into a virtual host stating that, if you are going to use the same password for all agent installations, you need to keep the same encryption key and the same encrypted password in the agent configuration file. For more information, see "Installing Apache Web Policy Agents into a Virtual Host" in the *Web Policy Agent Guide*.
	• Updated the `org.forgerock.openam.agents.config.policy.evaluation.realm` property reference to state that the property does not handle realm aliases. For more information, see Policy Client Service Properties in the *Web Policy Agent Guide*.

Date	Description
	• Added steps to check that Apache HTTP server has the appropriate permissions on specific directories. For more information, see "To Install the Web Policy Agent into Apache Virtual Hosts" in the *Web Policy Agent Guide*.
	• Updated the description for the `org.forgerock.agents.config.keepalive.disable` property. For more information, see Miscellaneous Custom Properties in the *Web Policy Agent Guide*.
	• Updated a question-answer troubleshooting entry on installing the policy agent on SELinux. For more information, see Solutions to Common Issues in the *Web Policy Agent Guide*.
	• Removed a paragraph that indicated that GLIBC_2.3 AGI must be supported for any installation of web policy agents on Linux. Any Linux runtime compatible with CentOS5 is supported.
	• Added a statement that `amlbcookie` cookie must be set up to the AM's server ID when you want web policy agents to communicate with an AM site configured behind a load balancer. For more information, see "Supporting Load Balancers" in the *Web Policy Agent Guide*.
	• Updated the description of the `org.forgerock.agents.config.notenforced.ipurl` property. For more information, see "Configuring Web Policy Agent Application Properties" in the *Web Policy Agent Guide*.
	• Updated the conditional URL example. For more information, see "Configuring Access Management Services Properties" in the *Web Policy Agent Guide*.
	• Updated the text to clarify that when installing the policy agent as a root user into Apache, the **agentadmin** command can change the directory ownership to the same user and group specified in the Apache configuration. For more information, see "To Install the Web Policy Agent into Apache" in the *Web Policy Agent Guide*.
	• Updated the procedure to enable SSL for the IIS agent. For more information, see "Important Changes to Web Agents Functionality".
	• Updated examples so that the **agentadmin --p** command does not contain double quotes UNIX. For more information, see "To Install the Web Policy Agent into Apache Virtual Hosts" in the *Web Policy Agent Guide*.
	• Updated the OpenSSL Libraries Location by Operating System table to indicate that if you are using AIX, then the OpenSSL libraries `libcrypto.so` and `libssl.so` are `LIBPATH` for AIX. For more information, see "Before You Install" in the *Web Policy Agent Guide*.
	• Updated the documentation to indicate that OWA properties are not available to the agents. For more information, see "Configuring Web Policy Agent Advanced Properties" in the *Web Policy Agent Guide*.
	• Updated the Troubleshooting section with a question on what to do when the default Apache welcome page appears instead of any custom error pages after

Date	Description
	an upgrade. For more information, see Solutions to Common Issues in the *Web Policy Agent Guide*.
2018-09-25	Updated the default value for the `org.forgerock.agents.config.tls` property to `-SSLv3 -TLSv1 -TLSv1.1`. For more information, see Bootstrap Properties in the *Web Policy Agent Guide*.
2016-09-20	Reorganization of web policy agent documentation
2016-12-02	4.1.0 Release
2017-05-19	Web Agents 4.1 documentation refresh, which includes the following updates: • NGINX Plus policy agent documentation added. For more information, see "*Installing Web Policy Agents in NGINX Plus*" in the *Web Policy Agent Guide*. • Updated the procedure to create an agent profile. For more information, see "Creating Agent Profiles" in the *Web Policy Agent Guide* • Added a procedure to upgrade web policy agents. For more information, see "*Upgrading Web Policy Agents*" in the *Web Policy Agent Guide*. • Updated the list of known issues for the release. For more information, see Web Agents 4.2.
2018-01-25	Web Agents 4.1 documentation refresh, which includes the following updates: • Clarified support for OpenSSL. For more information, see "Supported OpenSSL Versions". • Improved documentation on the `org.forgerock.agents.config.keepalive.disable` property. For more information, see Miscellaneous Custom Properties in the *Web Policy Agent Guide*. • Clarified support for Apache HTTP Server for Windows. For more information, see "Supported Operating Systems & Web Servers". • Improved documentation regarding the Conditional Login URL feature. For more information, see Login URL Properties in the *Web Policy Agent Guide*. • Improved documentation on the `org.forgerock.agents.config.tls` property. For more information, see Bootstrap Properties in the *Web Policy Agent Guide*. • Improved documentation regarding not-enforced IP client lists. For more information, see Not Enforced IP Processing Properties in the *Web Policy Agent Guide*. • Improved documentation regarding audit logging properties. For more information, see Audit Properties in the *Web Policy Agent Guide*. • Improved documentation for the `com.forgerock.agents.ext.url.validation.default.url.set` property. For more information, see Naming URL and Failover Properties in the *Web Policy Agent Guide*.

Date	Description
	• Improved POST data preservation properties documentation. For more information, see Post Data Preservation Properties in the *Web Policy Agent Guide*.
2018-05-08	Added IIS 8.5 to the list of supported platforms for Web Agents 4.1.x.

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, training 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.