Release Notes

/ Web Agents 5

Latest update: 5.0.1.1

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 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 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™ 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.

Chapter 1

What's New in Web Agents

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

Important

Before upgrading to Web Agents 5.x, consider the following points:

- Web Agents 5.x only support AM 5.5 and later.
- When working with Agents 5, AM 6 requires Web Agents 5.0.1 and later.
- Web Agents 5.x require the WebSocket protocol to communicate with AM. Both the web server and the network infrastructure must support the WebSocket protocol. For example, Apache HTTP server requires the `proxy_wstunnel_module` for proxying the WebSocket protocol.

  For more information, refer to your network infrastructure and web server documentation.
- Web Agents 5.x's configuration is considerably different from that of earlier versions. For example, if you were using custom login pages in an earlier version, you must enable a new property for backwards-compatibility.

  Read the Release Notes to understand the impact of the changes before upgrading.

1.1. Patch Releases

- Web Agents 5.0.1.1 Patch Release

  ForgeRock periodically issues patch releases with important fixes to bugs. Web Agents 5.0.1.1 is the latest patch release, targeted for Web Agents 5.0.1 deployments and can be downloaded from the *ForgeRock BackStage* website. To view the list of fixes in this release, see Web Agents 5.0.1.1.

  Note

  ForgeRock patch releases are aimed as a fast-track method to provide fixes to existing bugs. These fixes improve the functionality, performance and security of your deployment. No new features have been introduced.

Web Agents 5.0.1 is available for download and can be found at the *ForgeRock BackStage* website.

1.2. New Features

Web Agents 5.0.1

Web Agents 5.0.1 is a maintenance release containing key fixes and a new feature:

- **Support for Custom Redirection Login Pages**

  Starting from 5.0.1, Web Agents introduce a custom redirection login mode that supports:

  - Environments that already have customized login pages that expect user sessions to be stored in SSO tokens instead of in OIDC JWTs, whether these are XUI login pages or not.
  - Environments configured so the users cannot access the AM servers directly.
  - Environments configured so the custom login pages are not part of AM's XUI.

  To support the custom redirection login mode, Web Agents 5.0.1 include the following properties:

  - `org.forgerock.openam.agents.config.allow.custom.login`
  - OpenAM Login URL `com.sun.identity.agents.config.login.url` (this property was removed in Web Agents 5, and it has been reinstated)

  For more information, see "Redirection and Conditional Redirection" in the *User Guide*.

Web Agents 5

Web Agents 5 is a major release that includes new features, functional enhancements and fixes.

Important

Web Agents 5 only supports AM 5.5 and later. For more information, see "Platform Requirements".

- **Communication With AM Uses the OAuth 2.0 Authorization Framework**

  Web agents and AM exchange OpenID Connect JSON web tokens (JWTs) containing the information required to authenticate clients and authorize access to protected resources. The former method of communication, platform lower-level (PLL) calls, is no longer used.

  To ensure integrity, AM signs the JWTs with the `test` key alias by default. To change the signing key, see "Configuring Access Management Servers to Communicate With Web Agents" in the *User Guide*.

Web Agents 5 includes a new property, JWT Cookie Name (`org.forgerock.openam.agents.config.jwt.name`), that specifies the name of the cookie that holds the JWT on the user's browser. By default, this property is set to the value of `am-auth-jwt`. For more information, see Profile Properties in the *User Guide*.

- **Support for OpenSSL 1.1.0 Added**

  Unix and Linux Web Agents 5 support OpenSSL 1.1.0 libraries. For more information about OpenSSL supported versions, see "OpenSSL Requirements".

- **Support for Windows Server 2016 Added**

  Web Agents 5 adds support for Apache HTTP Server and Microsoft IIS web servers on Windows Server 2016.

  For more information about supported web servers, see "Platform Requirements".

- **Regular Expression Support for Conditional Login URL Redirection**

  Web Agents now support regular expressions to improve conditional login URL redirection. For more information, see the Regular Expression Conditional Login URL property in "Configuring Access Management Services Properties" in the *User Guide*.

- **Support for NGINX Plus R13 Added**

  Web Agents 5 adds support for NGINX Plus R13 on CentOS, RedHat Enterprise Linux, Ubuntu, and Oracle Linux.

  For more information about supported web servers, see "Platform Requirements".

- **Agent Fallback to Local Configuration Mode for Not-Enforced Lists**

  Web Agents 5 introduces a new property, `com.forgerock.agents.config.fallback.mode`, that specifies whether the web agent should read the configuration stored in the local `agent.conf` file when AM is not available.

  When enabled, the web agent allows traffic to resources specified in the not-enforced lists when AM is not available.

  For more information, see Miscellaneous Custom Properties in the *User Guide*.

- **Continuous Security**

  Because web agents are the first point of contact between users and your business applications, they can collect inbound requests' cookie and header information which an AM server-side authorization script can then process.

  For example, you may decide that only incoming requests containing the `InternalNetwork` cookie can access the intranet outside working hours.

Web agents introduce two properties related to continuous security:

- Continuous Security Cookies (`org.forgerock.openam.agents.config.continuous.security.cookies`)
- Continuous Security Headers (`org.forgerock.openam.agents.config.continuous.security.headers`)

For more information about these properties, see Continuous Security Properties in the *User Guide*.

1.3. Major Improvements

Web Agents 5

- **Improved Notification System**

  To receive notifications from AM, versions prior to Web Agents 5 required the administrator to configure bidirectional communication through load balancers, firewalls, and proxy servers. Web Agents 5 simplifies configuration by using the WebSocket protocol to keep long-running connections open with AM.

  Listeners defined in the Agent Notification URL property (`com.sun.identity.client.notification.url`) are only relevant to releases prior to version 5 and should be removed.

  Note

  When configuring IIS web agents with stateless sessions, you must delete any listeners defined in the `com.sun.identity.client.notification.url` property. For more information, see the known issues section.

  The web agent also includes a new property, Web Socket Connection Interval (`org.forgerock.openam.agents.config.balance.websocket.connection.interval.in.minutes`), to configure the time interval after which the agent reopens its WebSocket connection to the AM site. This property ensures that WebSocket connections from agents are spread across the AM site.

  For more information, see "Notification System" and Profile Properties in the *User Guide*.

- **Improvements in Cross-Domain Single Sign-On**

  Cross-domain single sign-on (CDSSO) includes the following improvements:

  - CDSSO now provides single sign-on (SSO) for AM and web agents configured in the same DNS domain and across DNS domains.

    CDSSO is the default and only SSO mode for web agents, which simplifies the configuration.

  - AM now provides CDSSO using the OAuth 2.0 protocol and the `oauth2/authorize` endpoint. The former method of providing SSO, `CDCServlet`, is no longer used.

Due to these changes, the following properties are no longer used:

- CDSSO Servlet URL (`com.sun.identity.agents.config.cdsso.cdcservlet.url`)
- Cross Domain SSO (`com.sun.identity.agents.config.cdsso.enable`)

For more information and implementation details, see About Single Sign-On and Configuring Cross-Domain Single Sign-On in the *ForgeRock Access Management Authentication and Single Sign-On Guide*.

- **Certificate Verification depth for OpenSSL Configurable**

  Web Agents 5 includes a new property, `org.forgerock.agents.config.cert.verify.depth`, that lets you specify the certificate verification depth when OpenSSL is enabled.

  For more information, see Encryption Properties in the *User Guide*.

- **Improved Audit Logging**

  Local and remote audit messages now adhere to the log structure common across the ForgeRock Identity Platform and support propagation of the transaction ID across the platform.

  For more information, see "Configuring Audit Logging" in the *User Guide*.

- **Improved Microsoft IIS Web Agent**

  The web agent for Microsoft IIS has been improved. You can now:

  - Install a web agent in the root of a site, in any application or sub-application of the IIS hierarchy.
  - Override a parent's application web agent configuration with a different web agent configuration.
  - Disable web agent protection the for root of a site, for any application or sub-application of the IIS hierarchy.

  For more information about installing web agents in Microsoft IIS, see "Installing the IIS Web Agent" in the *User Guide*.

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

The following security advisory concerns vulnerabilities that have been discovered in this release of Web Agents:

- Web Agents Security Advisory #201802. Fixed in Web Agents 5.0.0.1.

1.5. Patch Releases

Web Agents 5.0.0.3

- Web Agents 5.0.0.3 is a cumulative patch release containing key fixes. No new features have been introduced. For more information, see Web Agents 5.0.0.3.

Important

If you upgrade the AM server from OpenAM 12.0.x to AM 5.5.x, for example, existing agent profiles may not get fully migrated and a segmentation fault may occur. If the agent is likewise upgraded to the Agents 5 series prior to this 5.0.0.3 patch release and you have a local profile, update the `agent.conf` file and add the following parameters: `com.forgerock.openam.agents.config.jwt.name` and `com.sun.identity.agents.config.cdsso.redirect.uri`.

For example, add the properties with the value of the JWT and URI variables, respectively, which can be obtained from the AM admin console (Realms > *Realm Name* > Applications > Agents > Web > *Agent Name*) :

```
com.forgerock.openam.agents.config.jwt.name=am-auth-jwt
com.sun.identity.agents.config.cdsso.redirect.uri=agent/cdsso-oauth2
```

For a list of required properties, see "Configuration Location" in the *User Guide*.

Web Agents 5.0.0.2

- Web Agents 5.0.0.2 is a cumulative patch release containing key fixes. No new features have been introduced. For more information, see Web Agents 5.0.0.2.

Web Agents 5.0.0.1

- Web Agents 5.0.0.1 is a cumulative patch release containing a fix for a security vulnerability. No new features have been introduced.

Chapter 2

Before You Install

This chapter covers software and hardware prerequisites for installing and running web 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. Platform Requirements

The following table summarizes platform support.

Supported Operating Systems and Web Servers

Operating Systems	OS Versions	Web Servers & Versions
CentOS Red Hat Enterprise Linux Oracle Linux	6, 7	Apache HTTP Server 2.2, 2.4 NGINX Plus R12, R13
Microsoft Windows Server	2008 R2	Microsoft IIS 7.5 Apache HTTP Server 2.2, 2.4 [a]
	2012, 2012 R2	Microsoft IIS 8, 8.5 Apache HTTP Server 2.2, 2.4 [a]
	2016	Microsoft IIS 10 Apache HTTP Server 2.2, 2.4 [a]
Oracle Solaris x86 Oracle Solaris SPARC	10, 11	Apache HTTP Server 2.2, 2.4
Ubuntu Linux	14.04 LTS, 16.04 LTS	Apache HTTP Server 2.2, 2.4 NGINX Plus R12, R13
IBM AIX	6, 7	IBM HTTP Server 7, 9

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

Important

Web Agents 5.x require the WebSocket protocol to communicate with AM. Both the web server and the network infrastructure must support the WebSocket protocol. For example, Apache HTTP server requires the `proxy_wstunnel_module` for proxying the WebSocket protocol.

Refer to your network infrastructure and web server documentation for more information about WebSocket support.

2.2. Access Management Requirements

Web Agent 5 *does not* interoperate with:

- OpenAM
- AM versions earlier than 5.5.

2.3. OpenSSL Requirements

Agents require OpenSSL or the native Windows SSL libraries to be present. These libraries help to secure communications, for example when connecting to AM using websockets.

The following table summarizes OpenSSL support in Agents 5:

Supported OpenSSL Versions

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

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

Note

OpenSSL 1.0.2 or newer is required to support TLSv1.2

2.4. Other Requirements

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

Linux Systems

- Before installing Web agents on Linux, run the following command to make sure that `libc.so.6` is available, and that it supports the GLIBC_2.3 API:

```
$ strings libc.so.6 | grep GLIBC_2
```

- Web Agents on Linux systems require a minimum of 135 MB 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
```

- Web agents on Linux require a minimum of 16 MB of shared memory for the session and policy cache and the various worker processes and 140 MB shared memory for the logging system. Failure to provide enough shared memory may result in errors similar to the following:

```
2017-11-10 12:06:00.492 +0000   DEBUG [1:7521][source/shared.c:1451]am_shm_create2() about to create
 block-clusters_0, size 1074008064
2017-11-10 12:06:00.492 +0000   ERROR [1:7521]am_shm_create2(): ftruncate failed, error: 28
```

  To configure additional shared memory for the session and policy cache, see "Configuring Web Agent Environment Variables" in the *User Guide*.

- If POST data preservation is enabled, the web agent requires additional free disk space in the web agent installation directory to store the POST data cache files.

Microsoft Windows Systems

- Before installing the IIS web agent, 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 GB of free disk space at all times in the agent installation directory. If the amount of free space drops below this threshold, a warning similar to the following appears in the `agent.log` file:

```
016-11-10 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 web agent.

  Failure to free up disk space and restart the web 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)
```

- Web agents on Windows require a minimum of 16 MB of shared memory for the session and policy cache and the various worker processes and 140 MB shared memory for the logging system. Failure to provide enough shared memory may result in errors similar to the following:

```
2017-11-10 12:06:00.492 +0000   DEBUG [1:7521][source/shared.c:1451]am_shm_create2() about to create
 block-clusters_0, size 1074008064
2017-11-10 12:06:00.492 +0000   ERROR [1:7521]am_shm_create2(): ftruncate failed, error: 28
```

  To configure additional shared memory for the session and policy cache, see "Configuring Web Agent Environment Variables" in the *User Guide*.

- If POST data preservation is enabled, the web agent requires additional free disk space in the web agent installation directory to store the POST data cache files.

2.5. 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

Web Agents 5

- **SSO Cookies are not Deleted When Receiving an HTTP 403 Forbidden Status**

  Web Agent 4.x introduced the `org.forgerock.agents.config.cdsso.deny.cleanup.disable` property to control whether the web agent should delete SSO cookies after receiving an HTTP 403 forbidden status. By default, the policy agent deleted the cookies.

  Web Agents 5 neither deletes SSO cookies in this scenario nor allows configuring this behavior. Therefore, the `org.forgerock.agents.config.cdsso.deny.cleanup.disable property` property has been removed.

- **Procedure to Enable OpenSSL for Web Agents on Windows Changed**

  Earlier versions of the web agent on Windows used the `AM_SSL_SCHANNEL` environment variable as well as the `org.forgerock.agents.config.secure.channel.disable` property to enable OpenSSL.

  The environment variable is no longer supported and web agents use the native Windows libraries for SSL communications by default. To enable OpenSSL, see "Installing the Apache Web Agent" or "Installing the IIS Web Agent" in the *User Guide*.

- **Default Size of the Session and Policy Cache Changed**

  Earlier versions of the web agent configured a session and policy cache of 1 GB, which could be reduced to 16 MB by setting the `AM_MAX_SESSION_CACHE_SIZE` environment variable to `0`.

  Web Agents 5 configure a session and policy cache of 16 MB. The cache can take values from 1048576 bytes (1 MB) to 1073741824 bytes (1 GB), configurable by using the `AM_MAX_SESSION_CACHE_SIZE` environment variable. If set to `0`, the size defaults to 16 MB.

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

- **Changes to Naming URL and Failover Bootstrap Properties**

Web Agents 5 have changed the following naming URL and failover bootstrap properties:

- `com.forgerock.agents.ext.url.validation.level`

  Earlier versions of the web agent supported configuring a value of `0` to log in and out of AM to validate that the naming URL was valid. Web Agents 5 removes support for this value.

- `com.sun.identity.agents.config.naming.url`

  Earlier versions of the web agents specified a list of AM server URLs that the agent would check for AM naming validation. Those configurations assumed there was no load balancer between the web agent and the AM servers.

  Web Agents 5 do not validate AM's naming service since clients and agents should access AM 5.5 and later through a site URL (a load balancer). Therefore, you should specify in this property the URL of your AM site (or sites, if you have a disaster-recovery configuration).

- **Changes to Conditional Login**

  Web Agents 5 change the OpenAM Conditional URL (`com.forgerock.agents.conditional.login.url`) and the Regular Expression Conditional Login URL (`org.forgerock.agents.config.conditional.login.url` properties as follows:

  - Web Agents 5 authenticate to and log out users from the oauth2/authorize endpoint, which is not configurable. Therefore, to specify the realm or authentication module to which users should authenticate to, or log out from, add a conditional redirection rule. For example:

    ```
    example.com|https://openam.example.com:8443/openam/oauth2/authorize?realm=customers
    ```

  - Web Agents 5 let you configure conditional login redirection against any service or website in your environment.
  - Web Agents 5 conditional login let you match domains, subdomains, and paths in the incoming request URL in each rule.

  For more information, see Login URL Properties in the *User Guide*.

- **Changes to POST Data Preservation (PDP)**

  Web Agents 5 change POST data preservation as follows:

  - **Clients do not recover PDP information from an endpoint**

    Clients using web agents earlier than version 5 used the PDP endpoint `http://agent.host:port/dummypost/sunpostpreserve` to recover their PDP information after logging into AM.

    Web Agents 5 removes that endpoint and changes the PDP flow as follows:

    - Each unauthenticated form POST to a protected resource generates a unique random identifier. This identifier is handled as follows:

  - The agent places it into a cookie and provides the cookie to the client.
  - The agent sends it to AM along with the authentication request for the client.
- After authentication, AM returns the session for the client alongside with the unique identifier. If the client cannot provide the identifier (because the cookie is missing) or the identifier differs from the one returned by AM, the web agent denies access to the stored POST data.

  The unique identifier and the cookie protect the client against cross-site request forgery (CSRF) attacks by ensuring a request cannot be replayed after authentication unless it was originally sent in the same browser session within a finite time.

- **The `com.forgerock.agents.config.pdpuri.prefix` property is no longer used**

  Web agents of a version earlier than 5 required the `com.forgerock.agents.config.pdpuri.prefix` property in configurations where multiple web servers were behind a load balancer that directed traffic based on the request URI.

  Web Agents 5 do not use an endpoint to recover PDP data, and therefore this property is no longer required.

For more information about the POST data preservation cache and its properties, see "Caching Capabilities" in the *User Guide* and Post Data Preservation Properties in the *User Guide*.

3.2. Deprecated Functionality

Web Agents 5

- No features are deprecated in this release.

3.3. Removed Functionality

Web Agents 5

- **Removed Support for the Identity Membership Environment Condition in Policies**

  Web Agents 5 does not support policies configured with the Identity Membership(`AMIdentityMembership`) environment condition. Instead, configure the equivalent User & Group (`Identity`) subject condition. For more information, see the *ForgeRock Access Management Authorization Guide*.

- **Removed Support for Operating System Versions**

  Web Agents 5 does not support the following operating system versions:

- Red Hat Enterprise Linux 5
- CentOS 5
- Oracle Linux 5
- Windows Server 2008

- **Removed the `AM_MAX_SHARED_POOL_SIZE` Environment Variable**

  Web Agents 5 remove support for the `AM_MAX_SHARED_POOL_SIZE` environment variable. Earlier versions of the web agents used this variable to specify the maximun amount of shared memory the web agent should use.

  For more information about Web Agents 5 shared memory requirements, see "Other Requirements".

- **Removed Properties**

  Web Agents 5 removes support for the following configuration properties:

  - Override Notification URL (`com.sun.identity.agents.config.override.notification.url`)
  - Configuration Cleanup Interval (`com.sun.identity.agents.config.cleanup.interval`)
  - Agent Notification URL (`com.sun.identity.client.notification.url`)
  - CDSSO Servlet URL (`com.sun.identity.agents.config.cdsso.cdcservlet.url`)
  - Cross Domain SSO (`com.sun.identity.agents.config.cdsso.enable`)
  - `org.forgerock.agents.config.cdsso.deny.cleanup.disable`
  - OpenAM Login URL (`com.sun.identity.agents.config.login.url`)

    This property has been reinstated in Web Agents 5.0.1.

  - Load Balancer Setup (`com.sun.identity.agents.config.load.balancer.enable`)

  The properties are still available when creating a new agent profile in AM 5.5 to provide backwards-compatibility with earlier versions of the web agent.

Chapter 4

Fixes, Limitations, and Known Issues

4.1. Key Fixes

Web Agents 5.0.1.1

- AMAGENTS-1711: Setting Message level debug on the agent results in WARN level debug
- AMAGENTS-1717: Authenticated Page does not result in the User being set
- AMAGENTS-1736: When AM is behind reverse proxy uses multiple cookie domains agent is not able to login

Web Agents 5.0.1

- AMAGENTS-1598: The agent gives 403 response rather than redirect when token is invalid before notification is received
- AMAGENTS-1556: WPA5 crashes when running with local audit log mode enabled
- AMAGENTS-1552: WPA5 crashes on return from redirect when username contains UTF8 characters
- AMAGENTS-1551: WPA agentadmin --g option is changing empty xml element value
- AMAGENTS-1550: WPA5 doesn't encode white space in username for REST /users endpoint
- AMAGENTS-1537: Agent 5 does not have standard solution for custom login pages.
- AMAGENTS-1533: Web agent 5 is not working with AM6

Web Agents 5.0.0.3

- AMAGENTS-673: Session and Profile Attributes cookies/headers are not created
- AMAGENTS-1408: SIGSEGV when trying to install agent 5 with wrong AM version
- AMAGENTS-1461: Segv errors in IBM http7 server agent for AIX6/32 bit.
- AMAGENTS-1479: AIX-7 IHS-9 64bit logs spurious errors, incomplete websocket frames and mishandles the error.

- AMAGENTS-1485: Agent 5 background threads are not entirely independent in different container instances
- AMAGENTS-1489: 32 bit sparc agents produce errors with SysV semaphore operations
- AMAGENTS-1509: Agent5 is crashing with unchecked use of r->conf->redirect_uri value
- AMAGENTS-1510: Agent5 is crashing with unchecked use of r->conf->jwt_name value
- AMAGENTS-1511: Agent5 is crashing on Apache for Windows server shutdown
- AMAGENTS-1523: Agent 5 websockets fail to reset correctly after ping failure
- AMAGENTS-1527: Crash in windows iis agent json handling

Web Agents 5.0.0.2

- AMAGENTS-1339: agentadmin --g crash on 4.1.0-27
- AMAGENTS-1402: Agent 5.0 config change notification intermittently fails to affect all worker processes.
- AMAGENTS-1436: Cannot install A5 with non-datastore module in default chain
- AMAGENTS-1439: nginx agent 5 rewrites https protocol to http

Web Agents 5

- AMAGENTS-1029: Ignore Path Info is ignored although NEU rule does not contain wildcard
- AMAGENTS-778: w3wp crashes in am_shm_lock
- AMAGENTS-705: Unauthorized POST data stay forever in agent, if you do not login
- AMAGENTS-621: Upgrade third party http_parser libs to 2.7.1
- AMAGENTS-620: wnet_read can cause potentially infinitely loop if E_AGAIN received
- AMAGENTS-509: 1 CPU used per w3wp process caught in loop in read_retry
- AMAGENTS-461: The agent does not do PDP for session upgrade.
- 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-370: FQDN mapping broken on varnish
- AMAGENTS-364: agents.config.policy.evaluation.realm does not handle realm aliases

- 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-311: Increase maximum URI size to 8k
- 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-278: Policy Agent is generating the cookies and headers, if one of the Attributes processing is Cookie and one of the Attribute Map is not empty.
- 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-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-229: protocol/port/host override don't work with Post Data Preservation
- AMAGENTS-217: Configurable depth for certificate verification
- AMAGENTS-214: agent.log is set to debug level and it is not possible to change it
- AMAGENTS-208: Agent returns HTTP 500 internal error on logout page if com.sun.identity.agents.config.logout.url map is empty
- AMAGENTS-207: Accessing the agent logout URL without session will cause a redirect
- AMAGENTS-181: Memory leak in case of network connection failure
- AMAGENTS-176: WPA4/3.x does not support policy.evaluation.application config property
- AMAGENTS-173: WPA4 on AIX does not work with a new logger
- AMAGENTS-172: WPA4 does not handle oversized log messages properly
- AMAGENTS-169: RFE: Don't depend on Apache's 'pathinfo'

- AMAGENTS-164: Agent with remote audit logger enabled and a little more than 4K messages agent will crash
- AMAGENTS-147: Agentadmin stops in OpenAM server validation phase
- AMAGENTS-144: Apache http server 2.2 crashes on Linux systems hosted on VirtualBox
- AMAGENTS-140: WPA is not using agents.config.polling.interval configuration property
- AMAGENTS-135: WPA4 running on Schannel might not read complete HTTP response body
- AMAGENTS-132: WPA is not able to recover from XML parser error
- AMAGENTS-130: IIS agent can crash in get_request_url method
- AMAGENTS-121: Web Agent not updating headers when AM Session Attributes are changed
- AMAGENTS-119: Windows Apache Agent crashes under load when constantly recycled
- AMAGENTS-105: IIS Agent Crash at read of log variable after destruction by another thread at application pool recycle
- AMAGENTS-103: Agent4 does not work well with mod_autoindex generated pages
- AMAGENTS-95: Improve Agent error handling of AM responses after OPENAM-8910
- AMAGENTS-93: RFE: file permissions and/or ownership of log files should be configurable
- AMAGENTS-68: invalid cookie causes 403 instead of redirect to login page
- AMAGENTS-52: WPA on Windows should be able to use Schannel for SSL/TLS communication
- AMAGENTS-49: WPA does not support IBM HTTP Server
- AMAGENTS-47: Agent truncates filtered HTTP POST body
- 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
- AMAGENTS-24: Non-enforced URL validation should be lazy
- AMAGENTS-19: IIS agent should support mixed 32 and 64 bit application pools
- AMAGENTS-1: WPA4 reads in only a limited set of session service attributes

4.2. Limitations

The following limitations and workarounds apply to Web Agent 5:

- **Ignore Path Info Properties Is not Supported for NGINX Plus Agent**

  The NGINX Plus web agent does not support the following ignore path info properties:

  - `com.sun.identity.agents.config.ignore.path.info`
  - `com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list`

- **IIS Web Agents May Fail to Install When IIS Configuration Is Locked**

  Installing web agents in IIS may fail with an error similar to the following:

  ```
  Creating configuration...
     Error: failed to create module entry for MACHINE/WEBROOT/APPHOST/AgentSite/ (error 0x80070021, line:
   1823).
     The process cannot access the file because another process has locked a portion of the file. (error:
   0x21).
     Installation failed.
  ```

  This error message means the **agentadmin.exe** command cannot access some IIS configuration files because they are locked.

  To work around this issue, perform the following steps:

  1. Open the IIS Manager and select the Configuration Editor.
  2. Unlock the IIS `system.webServer/modules` module.
  3. Retry the web agent installation.

  Note

  Unlocking the `system.webServer/modules` module should allow the installation to finish. However, you may need to unlock other modules depending on your environment.

- **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 5.0.0.1

- AMAGENTS-1408: SIGSEGV when trying to install agent 5 with wrong AM version
- AMAGENTS-1339: agentadmin --g crash on 4.1.0-27

Web Agents 5

- **IIS Web Agent With Stateless Sessions Returning HTTP 403 Errors When Accessing Protected Resources**

  IIS web agents configured for stateless sessions will return HTTP 403 errors when trying to access a protected resource if the `com.sun.identity.client.notification.url` property is configured.

  The `com.sun.identity.client.notification.url` property, used by earlier versions of the web agents to specify the notification listener for the agent, is not used or required for Web Agents 5. However, to provide backwards-compatibility with earlier versions of the agents, AM populates this property when creating the agent profile.

  The value of this property should removed for all web agents 5 installations, and must be removed for IIS Web Agents 5 configured for stateless sessions.

- **Install IIS Web Agents on Child Applications Before Installing in Parent Application**

  In an IIS environment where you need to protect a parent application and a child application with different web agent configurations, you must install the web agent on the child application before installing the web agent in the parent. Trying to install a web agent on a child that is already protected will result in error.

- **agentadmin --v Command Does Not Reflect Web Agents 5 Shared Memory Requirements**

  The system resources output from the **agentadmin --v** command does not reflect Web Agents 5 shared memory requirements. For more information, see "Other Requirements".

- **Default Welcome Page Showing After Upgrade Instead of Custom Error Pages**

  After upgrading, you may see the default Apache welcome pages instead of custom error pages defined by the Apache `ErrorDocument` directive.

  If you encounter this issue, check your Apache `ErrorDocument` configuration. If the custom error pages are not in the document root of the Apache server, you should enclose the `ErrorDocument` directives in `Directory` elements. For example:

  ```
  <Directory "/web/docs">
     ErrorDocument 403 myCustom403Error.html
  </Directory>
  ```

  Refer to the Apache documentation for more details on the `ErrorDocument` directive.

- AMAGENTS-1319: Changing debug log level in agent profile has effect for background tasks agent.log file
- AMAGENTS-1310: When we install the agent manually on Ubuntu Apache, the installer does not change permissions on the agent files
- AMAGENTS-1295: Can not disable configuration change notifications with Solaris Agent

- AMAGENTS-1267: org.forgerock.agents.config.secure.channel.disable should be in agent.conf by default
- AMAGENTS-1252: It is not possible to install an IIS agent for child application, if one agent instance is installed for parent application/site
- AMAGENTS-1240: Decrease log level for incorrect JWT token in Agent 5
- AMAGENTS-1188: com.forgerock.agents.ext.url.validation.default.url.set does not use the primary url as expected
- AMAGENTS-1185: url.validation.ping.interval does not work for C Agent 5
- AMAGENTS-1174: Files are left over in tmp directory after apache has been switched off
- AMAGENTS-1156: Disabled "Agent Configuration Change Notification" does not work properly, if new worker is created for C Agent
- AMAGENTS-1123: Unused property (com.forgerock.agents.init.retry.max) in Agent 5
- AMAGENTS-1104: IIS Agent installer gives error messages about ssleay32.dll and libeay32.dll not being available
- AMAGENTS-1039: If C Agent Policy Client Service - Realm does not have a slash at the start the realm value is not understood by the C Agent
- AMAGENTS-800: Headers not being logged as part of the remote audit log
- AMAGENTS-523: The files created during installation (e.g agent.conf) have the wrong permissions
- AMAGENTS-456: URL Comparison Case Sensitivity Check does not work for policies

Chapter 5
Documentation Updates

The following table tracks changes to the documentation set following the release of AM Web Agent 5:

Documentation Change Log

Date	Description
2018-09-25	Updated the default value for the `org.forgerock.agents.config.tls` property to `-SSLv3 -TLSv1 -TLSv1.1`. .
2019-09-20	Labelled documentation relating to support for Domino servers as unused, as support was removed from Web Agent 4 and later.
2018-09-19	Release of Web Agents 5.0.1.1 patch release. Removed the Load Balancer Setup (`com.sun.identity.agents.config.load.balancer.enable`) property from the documentation. Added an entry in the troubleshooting section on handling Error 24 issues. For more information, see Solutions to Common Issues. Removed obsolete OWA properties. for more information, see Microsoft IIS Server Properties in the *User Guide*.
2018-05-08	Added IIS 8.5 to the list of supported platforms
2018-05-02	Maintenance release of Web Agents 5.0.1
2018-03-16	Patch release of Web Agents 5.0.0.3
2018-02-16	Patch release of Web Agents 5.0.0.2
2018-01-18	Patch release of Web Agents 5.0.0.1
2017-12-20	First release of Web Agents 5

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 on ForgeRock's support offering, including support plans and service level agreements (SLAs), visit https://www.forgerock.com/support.