FORGEROCK®

Release Notes
/ Web Agents 5.6

Latest update: 5.6.3

Copyright © 2011-2020 ForgeRock AS.

Abstract

Notes covering prerequisites, fixes, known issues for ForgeRock® Access Management web 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 5.6.x, consider the following points:
>
> • Web Agents 5.6.x only supports AM 5.5 and later.
>
> • Web Agents 5.6.x requires 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.
>
> • If you are upgrading from a version earlier than 5, Web Agents 5 introduced notable changes in the configuration. For example, if you are using custom login pages, you must enable the `org.forgerock.openam.agents.config.allow.custom.login` property. For more information about changes introduced in Web Agents 5, refer to the Web Agents 5 Release Notes.

Maintenance Releases

ForgeRock maintenance releases contain a collection of fixes and minor RFEs 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 5.6.3

• Web Agents 5.6.3 is the latest release targeted for Web Agents 5.6.x deployments, and can be downloaded from the *ForgeRock Backstage* website.

  See the list of fixes here.

New Features

Web Agents 5.6.3

• Changes to the Custom Login Redirection Mode

Previous versions of Web Agents included the the Exchange SSO Token for JWT (com.forgerock.agents.accept.ipdp.cookie) property, which was used to convert SSO tokens into ID tokens during the custom login redirection mode.

Web Agents 5.6.3 makes this property legacy, and includes a new property to replace it, Accept SSO Token (`com.forgerock.agents.accept.sso.token`).

For more information about the new property, see Accept SSO Token (Not yet in the AM console)[2] in the *User Guide*.

Web Agents 5.6.2.1

• There are no new features in this release, only bug fixes.

Web Agents 5.6.2.0

• Disable Validation of the `aud` and `nonce` JWT Claims

During an authentication request, AM creates a JWT that contains, among others, the end user's session and the `aud` claim. This claim is set to the agent profile of the agent that made the request. When AM returns the JWT to the end user's user-agent, it appends to the request a `nonce` parameter, which is a one-time-usable random string that is understood by both AM and the agent that made the authentication request.

When the agent receives a request to access a protected resource and the end user's user-agent attaches the JWT and the `nonce` parameter to the request, the agent checks that both the audience of the JWT (the `aud` claim) and the value of the `nonce` parameter are appropriate. For example, it checks that the value of the `aud` claim is the name of its own agent profile.

In environments where several agents protect the same application, this validation poses a problem; even if the JWT is valid and contains a valid session, an agent cannot validate a JWT created for a different agent since the audience and the `nonce` would not match. Therefore, the agent redirects the end user for authentication again.

Web Agents 5.6.2 introduces the following advanced properties to disable the validation of the `aud` and `nonce` claims represented in the JWT:

• `com.forgerock.agents.jwt.aud.whitelist`. Configure a comma-separated list of agent profile IDs that the agent will accept as valid values for the `aud` claim.

Use this property, for example, when your agents are configured with different agent profiles yet they are protecting the same application.

Configuring this property disables `nonce` validation.

- `com.forgerock.agents.jwt.aud.disable`. Set this property to `1` to stop the agent from validating both the `aud` and `nonce` claims.

  > **Note**
  >
  > Agents should validate as many claims as possible for security reasons. Configure this property only if the `com.forgerock.agents.jwt.aud.whitelist` property is not suitable for your environment.

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

- Allow Agents to Refresh Session's Idle Timeout When Configured in SSO-only Mode

  Sessions in AM have an idle timeout after which they expire. In general, when users access protected resources through an agent, the agent requests a policy decision on behalf of that user, which resets the idle timeout.

  If the agent is configured in SSO-only mode, the session may unexpectedly expire in AM due to idle timeout before the user has finished accessing the application.

  To force the agent to refresh the users' session idle timeout when the user performs an action, Web Agents 5.6.2 includes the new `com.forgerock.agents.call.session.refresh` property.

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

- New Configuration Option for the `org.forgerock.openam.agents.config.allow.custom.login` Property

  Web Agents 5.6.2 adds a new configuration option for the `org.forgerock.openam.agents.config.allow.custom.login` property that appends a `goto=original_request_url` parameter to the redirect URL.

  For more information, see "Custom Login Redirection Mode" in the *User Guide*.

Web Agents 5.6.1.1

- There are no new features in this release.

Web Agents 5.6.1.0

- Support for Public AM URLs

  Web Agents 5.6.1.0 includes a new property, `com.forgerock.agents.public.am.url`, that specifies the public URL of the AM to redirect to. Use this property in environments where custom login pages

are in a network that can only access AM using a proxy, a firewall, or any other technology that remaps the AM URL to one accessible by the custom login pages.

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

• Support for Converting SSO Tokens into OpenID Connect JWTs

Web Agents 5.6.1.0 includes a new property, `com.forgerock.agents.accept.ipdp.cookie`, that specifies whether the agent should convert SSO tokens (iPlanetDirectoryPro cookies) present on requests into OpenID Connect JWTs.

Set this property when your end users access resources protected by both Web Agents 4.x (which use SSO tokens) and 5.x (which use OpenID Connect JWTs). Converting the SSO token to a JWT will ensure a seamless experience to the user without additional redirection or re-authentication.

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

Web Agents 5.6.0

Web Agents 5.6.0 is a minor release that includes new platform support, bug fixes, and a new feature:

• Added Support for Distributed Policy Evaluation

Web Agents 5.6.0 introduces a policy cache, which builds upon the existing policy decision cache.

When enabled, web agents download and store details about policies from AM, and use them to make authorization decisions without having to contact AM each time. This reduces the agents' callbacks to AM and can increase the performance of the agents.

> **Important**
>
> This functionality is a Technology Preview.

For more information, see "Caching Capabilities" in the *User Guide*.

• Support for TLSv1.3 added

Web Agents 5.6 introduces support for TLSv1.3. OpenSSL 1.1.1 or later is required to support this protocol.

For more information about supported OpenSSL versions, see "OpenSSL Requirements".

Major Improvements

Web Agents 5.6.3

• AMAGENTS-2720: Request for a Cache for SSO tokens, to allow Agent 5+ to use only cookies

FORGEROCK

Web Agents 5.6.2.1

- There are no new feature improvements in this release, only bug fixes.

Web Agents 5.6.2.0

- Changes in MIME-Encoding of HTTP Header Values

  Earlier versions of Web Agents MIME-encoded HTTP header values if said values were multi-byte unicode strings.

  Web Agents 5.6.2 introduces a new advanced property, `com.forgerock.agents.header.mime.encode`, that controls whether the agent should MIME-encode the value of the HTTP headers, and when.

  The default value of the new property honors the behavior of previous releases.

  For more information, see Miscellaneous Header-Related Properties in the *User Guide*.

- **Re-Introduction of `goto` Parameter for Custom Login Redirect**

  Web Agents 5.6.2.0 has re-introduced the `goto` parameter for custom login redirects in IPDP mode.

  To set this feature, set the following properties:

  - `org.forgerock.openam.agents.config.allow.custom.login`=2

  - `com.forgerock.agents.accept.ipdp.cookie`=1 (or 2), where 1 enables the feature to accept IPDP cookies, or 2 accepts IPDP cookies and realms.

- **New Option to Change Advice Format Value**

  Web agents 5.6.2.0 introduces a new property, `com.forgerock.agents.advice.b64.url.encode=1`, which changes the advice format XML, sent as part of the composite advice by the agent to AM. When the property is enabled, the advice is sent as base64url-encoded data.

  For more information, see AMAGENTS-2973: Create option to Change Advice Format Value

Web Agents 5.6.1.1

- There are no new improvements in this release, only bug fixes.

Web Agents 5.6.1.0

- There are no new improvements in this release, only bug fixes.

FORGEROCK

Web Agents 5.6.0

- There are no new improvements in this release, only bug fixes.

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.

Platform Requirements

The following table summarizes platform support.

Supported Operating Systems and Web Servers

Operating Systems	OS Versions	Web Servers & Minimum Supported Versions
Amazon Linux 2, CentOS, Oracle Linux, Red Hat Enterprise Linux	6, 7	Apache HTTP Server 2.4, IBM HTTP Server 9.0, NGINX Plus R16, NGINX Plus R17
IBM AIX	6, [b] 7	IBM HTTP Server 9
Microsoft Windows Server	2008 R2 [b]	Apache HTTP Server 2.4, [a] Microsoft IIS 7.5
	2012, [b] 2012 R2 [b]	Apache HTTP Server 2.4, [a] Microsoft IIS 8, Microsoft IIS 8.5
	2016	Apache HTTP Server 2.4, [a] Microsoft IIS 10
Oracle Solaris SPARC, Oracle Solaris x64	10, 11	Apache HTTP Server 2.4
Ubuntu Linux	16.04 LTS, [b] 18.04 LTS	Apache HTTP Server 2.4, NGINX Plus R16 (NGINX open source build 1.15.2), NGINX Plus R17 (NGINX open source build 1.15.7)

[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.
[b] Support for this platform will be discontinued in a future release.

> **Important**
>
> 1. Web Agents 5.6.3 requires 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. Support for 32-bit architectures on Unix-based platforms will be discontinued in a future release.

Access Management Requirements

Web Agent 5.6.3 *does not* interoperate with:

• OpenAM

• AM versions earlier than 5.5.

OpenSSL Requirements

Agents require OpenSSL or the Windows built-in Secure Channel API to be present. These libraries help to secure communications, for example, when connecting to AM using the WebSocket protocol.

The following table summarizes OpenSSL support in Agents 5.6.3:

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, OpenSSL 1.1.0, OpenSSL 1.1.1 [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 web agents use the Windows built-in Secure Channel API by default.

> **Important**
>
> 1. OpenSSL 1.0.2 or later is required to support TLSv1.2. If you have to use an earlier, *weaker* cipher in your environment, configure the `org.forgerock.agents.config.tls` bootstrap property with a security protocol other than TLSv1.2.
>
> 2. OpenSSL 1.1.1 or later is required to support TLSv1.3.

Other Requirements

Before installing web agents on your platform, also 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 require a minimum of 16 MB of shared memory for the session and policy cache and the various worker processes and additionally, 32 KB 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. To change the POST data storage directory, see Post Data Preservation Properties in the *User Guide*.

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 require a minimum of 16 MB of shared memory for the session and policy cache and the various worker processes in the system page file and additionally, 32 KB 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. To change the POST data storage directory, see Post Data Preservation Properties in the *User Guide*.

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.

Important Changes to Existing Functionality

Web Agents 5.6.3

• Property and Value Pairs Set as Advanced Properties Are the Source of Truth

  Web Agents 5.6.3 take properties and value pairs set as advanced properties as the source of truth for that property. Earlier versions of the agents used the value in the property as the source of truth.

  For example, if you configure the value of the JWT Cookie Name property in the AM UI, but you also configure `org.forgerock.openam.agents.config.jwt.name=myJWT` as an advanced property, the agent now uses the latter, even if both are configured.

Web Agents 5.6.2.1

• There are no major changes in functionality in this release, other than bug fixes.

Web Agents 5.6.2.0

• There are no major changes in functionality in this release, other than bug fixes.

Web Agents 5.6.1.1

• There are no major changes in functionality in this release, other than bug fixes.

Web Agents 5.6.1.0

• Changes to the **agentadmin --V** Command

  Earlier versions of Web Agents included the **agentadmin --V** command, which you can use to validate an agent instance configuration.

As part of the validation process, the **agentadmin** command ensures that the core init and shutdown agent sequences are working as expected. In some situations, this check made the agent instance unresponsive, causing unexpected service outages.

Web Agents 5.6.1.0 does not execute the init and shutdown sequences when using the `--V` option. To run them, use the `--Vi` option instead.

For more information, see "Command-Line Tool Reference" in the *User Guide*.

Web Agents 5.6.0

- Fully Qualified Domain Name Checking Off by Default

  The `com.sun.identity.agents.config.fqdn.check.enable` is now set to `false` by default. This default value was changed for the 5.6.0 release and differs from previous releases, which was set to `true`. The change better aligns local configurations to be consistent with centralized profiles, which has FQDN checking off by default.

Deprecated Functionality

Web Agents 5.6.3

- No functionality has been deprecated in this release.

Web Agents 5.6.2.1

- No functionality has been deprecated in this release.

Web Agents 5.6.2.0

- No functionality has been deprecated in this release.

Web Agents 5.6.1.1

- No functionality has been deprecated in this release.

Web Agents 5.6.1.0

- No functionality has been deprecated in this release.

Web Agents 5.6.0

- No functionality has been deprecated in this release.

Removed Functionality

Web Agents 5.6.3

• No components were removed in this release.

Web Agents 5.6.2.1

• No components were removed in this release.

Web Agents 5.6.2.0

• No components were removed in this release.

Web Agents 5.6.1.1

• No components were removed in this release.

Web Agents 5.6.1.0

• No components were removed in this release.

Web Agents 5.6.0

• No components were removed in this release.

Chapter 4

Fixes, Limitations, and Known Issues

Key Fixes

Web Agents 5.6.3

- AMAGENTS-1610: If we set a property in the Custom Properties, it should overwrite value from other part of GUI

- AMAGENTS-2711: Fix nginx agent authentication under http/2 connections

- AMAGENTS-2728: Agent5 will not redirect to AMPostAuthProcessInterface.POST_PROCESS_LOGIN_SUCCESS_URL value

- AMAGENTS-3163: Web Agent audit log lines entries are truncated at 4096 bytes

- AMAGENTS-3205: Allow to set SameSite cookie attribute in web agent

- AMAGENTS-3303: Fallback mode does not work reliably

- AMAGENTS-3368: Webagent on 32bit windows platform will crash while opening existing log file which is close to (or over) 2GB in size

- AMAGENTS-3382: (WPA) Redirect loop is possible in custom login mode 1/2 because invalid sso cookie is not removed

- AMAGENTS-3404: Webagent 5 should display/log Cookie header value in validate_token

Web Agents 5.6.2.1

- AMAGENTS-2976: NEU Attribute fetch does not work unless there is cached data already.

- AMAGENTS-3056: The agent does not invalidate session before redirecting to logout

- AMAGENTS-3096: Realm argument within validator description negates the required slash

- AMAGENTS-3134: Invalid configuration of postdata.preserve.dir leads to crash / segmentation fault

Web Agents 5.6.2.0

- AMAGENTS-1370: port XHOST forwarding into web agents (apache agent & iis)

- AMAGENTS-2510: Agent5 running in SSO only mode is not using session response TTL values for its cache entry

- AMAGENTS-2699: Use whitelist to determine if jwt audience is allowed for agent

- AMAGENTS-2762: Agent is not mime-encoding specific UTF-8 header value

- AMAGENTS-2816: WPA5 is using hardcoded socket read timeout value for Windows SSL handshake processing module

- AMAGENTS-2840: WebAgent performs AM user REST call, although not needed

- AMAGENTS-2842: Re-introduce goto parameter handling for custom login redirect in web agent.

- AMAGENTS-2885: session SDK REST call to /users?_fields does not handle 404/400 as a valid rest/user json response

- AMAGENTS-2910: Not enforce requests containing particular cookie or header

- AMAGENTS-2975: Agent 5 not encoding # sign

- AMAGENTS-2982: Integer overflow error in http_request_serialise_host

- AMAGENTS-2998: Cannot access allowed site with agent using http

- AMAGENTS-3006: Drop of 25% in mean request per second time for Rest Fixed Performance Test for IIS platform

- AMAGENTS-3036: Windows CNG hashing code is not compatible with Windows 2008R2

- AMAGENTS-3095: Agent crashes parsing json object over 4096 bytes

Web Agents 5.6.1.1

- AMAGENTS-2816: WPA5 is using hardcoded socket read timeout value for Windows SSL handshake processing module

- AMAGENTS-2798: Seg Fault when custom login=true but login.url is empty

Web Agents 5.6.1.0

- AMAGENTS-2678: sso cookie is not found on custom-login-response and requires us to customize the service url

- AMAGENTS-2684: Create arg on Validator to not initiate validate_worker_init_shutdown.

- AMAGENTS-2702: If an sso token is presented, optimise agent flow by oauth2 token exchange

Web Agents 5.6.0

- AMAGENTS-215: FQDN checking should be turned off by default - Web agent local file

- AMAGENTS-1264: Update IIS agent Basic Auth support for JwtPasswordReplay

- AMAGENTS-1861: Agent 5 crash in websocket_handshake on Solaris SPARC

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

- AMAGENTS-2188: Replace use of non-threadsafe strerror

- AMAGENTS-2199: Port override does not work properly when agent is behind load balancer

- AMAGENTS-2407: Agent is resetting CDSSO session cookie on authn redirect with policy advice available

- AMAGENTS-2456: WPA for Windows does not support OpenSSL 1.1.x

Limitations

Web Agents 5.6.3

- The **agentadmin** Command Shows Warning Messages When Using JDK 11

  The `agentadmin` command may show warning messages similar to the following when using JDK 11. You can safely ignore these messages:

```
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.forgerock.openam.sdk.com.google.inject.internal.cglib.core.
$ReflectUtils$1 ...
WARNING: Please consider reporting this to the maintainers of
 org.forgerock.openam.sdk.com.google.inject.internal.cglib.core.$ReflectUtils$1
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
```

- AMAGENTS-2720: Request for a Cache for SSO tokens, to allow Agent 5+ to use only cookies. Note: This fix works with AM 6 or later.

- AMAGENTS-3382: (WPA) Redirect loop is possible in custom login mode 1/2 because invalid sso cookie is not removed. Note: This fix works with AM 6 or later.

Web Agents 5.6.2.1

- Remote Audit Logging May Decrease Throughput

  Testing has found that use of remote audit logging may impact performance throughput due to the large number of requests sent from the web agent to AM.

Web Agents 5.6.2.0

- There are no known limitations or workarounds in this release.

Web Agents 5.6.1.1

• There are no known limitations or workarounds in this release.

Web Agents 5.6.1.0

• There are no known limitations or workarounds in this release.

Web Agents 5.6.0

• There is no deprecated functionality in this release.

Known Issues

Web Agents 5.6.3

• There are no new known issues in this release.

Web Agents 5.6.2.1

• There are no new known issues in this release.

Web Agents 5.6.2.0

• There are no new known issues in this release.

Web Agents 5.6.1.1

• There are no new known issues in this release.

Web Agents 5.6.1.0

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

• AMAGENTS-523: The files created during installation (e.g agent.conf) have the wrong permissions

• AMAGENTS-1584: Error message is confusing if using a different realm for obtaining the ID token compared with the SSO token

• AMAGENTS-2164: When setting audit log location to REMOTE there is a huge drop in performance

• AMAGENTS-2617: Build machine value is missing in version output for centos 7 nginx builds

Web Agents 5.6.0

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

- AMAGENTS-523: The files created during installation (e.g agent.conf) have the wrong permissions

- AMAGENTS-1584: Error message is confusing if using a different realm for obtaining the ID token compared with the SSO token

- AMAGENTS-2164: When setting audit log location to REMOTE there is a huge drop in performance

- AMAGENTS-2617: Build machine value is missing in version output for centos 7 nginx builds

Chapter 5
Documentation Updates

The following table tracks changes to the documentation set following the release of AM Web Agent 5.6:

Documentation Change Log

Date	Description
2020-11-18	Initial release of Web Agents 5.6.3. The following documentation updates were made: • Updated the documentation to indicate that `prefork-mpm` should not be configured, as it may cause performance issues to both the agent and AM. See "Tuning Apache Multi-Processing Modules" in the *User Guide*. • Updated the documentation for the session invalidate property. See Logout URL Properties in the *User Guide*. • Updated the documentation to emphasize that the Profile Attribute Map property is case-sensitive and must match the schema exactly. See Profile Attributes Processing Properties in the *User Guide*.
2020-02-03	Initial release of Web Agents 5.6.2.1. The following documentation updates were made: • Added documentation about the new configuration option for the `org.forgerock.openam.agents.config.allow.custom.login` property and its release note for the 5.6.2.0 release. For more information, see Web Agents 5.6.2.0. • Added documentation about restrictions on children applications for a parent's or site's IIS configuration. For more information, see "Before You Install" in the *User Guide*.
2019-11-05	Initial release of Web Agents 5.6.2.0 The following documentation updates were made: • Added documentation on two new properties, `com.forgerock.agents.jwt.aud.whitelist` and `com.forgerock.agents.jwt.aud.disable`. For more information, see General Properties in the *User Guide*. • Updated the documentation of the `com.sun.identity.agents.config.local.log.size` property. For more information, see "Configuring Audit Logging" in the *User Guide*.

Date	Description
	The descriptions for the `Rotate Local Audit Log` and `Local Audit Log Rotation Size` properties were updated. For more information, see "Configuring Global Properties" in the *User Guide*.
	• Updated the description of the `Regular Expression Conditional Login URL` by specifying the string and pipe are not required for regular expression conditional login rules. For more information, see Login URL Properties in the *User Guide*.
	• Removed references to IBM Lotus Domino Server properties. This server is no longer supported.
	• Updated documentation with TLSv1.3 support. OpenSSL 1.1.1 or later is required. For more information, see "OpenSSL Requirements".
2019-09-20	Labelled documentation relating to support for Domino servers as unused, as support was removed from Web Agent 4 and later.
2019-09-06	Documented the method for specifying the HTTP method that must be used in conjunction with the URL in a not-enforced rule. For example, you may want to allow all HTTP OPTIONS requests to your `/scripts/` folder.
	For more information, see "Not-Enforced URL and Client IP Lists" in the *User Guide*.
2018-08-11	Initial release of Web Agents 5.6.1.1.
2019-07-04	Initial release of Web Agents 5.6.1.0.
	The following documentation updates were made for this release:
	• Added documentation about the requirement to validate WebSocket communication between your web server and AM. For more information, see "To Install the Apache Web Agent" in the *User Guide*, "To Install the IIS Web Agent" in the *User Guide*, or "To Install the NGINX Plus Web Agent" in the *User Guide*.
	• Added a new property, `com.forgerock.agents.public.am.url.property`. For more information, see Login URL Properties in the *User Guide*.
	• Added a new property `com.forgerock.agents.accept.ipdp.cookie` property. For more information, see Profile Properties in the *User Guide*.
	• Added documentation on **agentadmin** command's validation mode, `--V[i]` option. For more information, see agentadmin(1) in the *User Guide*.
	• Added a new property, `com.forgerock.agents.accept.ipdp.cookie`. For more information, see Profile Properties in the *User Guide*.
2019-03-29	Initial release of Web Agents 5.6.0.

Appendix A. Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

ForgeRock Product Release Levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

Release Level Definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated • Include changes present in previous Minor and Maintenance releases
Minor	Version: x.y[.0] (trailing 0s are optional)	• Bring minor features, and bug fixes

Release Label	Version Numbers	Characteristics
		• Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces • Can remove previously Deprecated functionality • Include changes present in previous Minor and Maintenance releases
Maintenance, Patch	Version: x.y.z[.p] The optional `.p` reflects a Patch version.	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release

ForgeRock Product Stability Labels

ForgeRock products support many features, protocols, APIs, GUIs, and command-line interfaces. Some of these are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these features and interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines stability labels and uses these definitions in ForgeRock products.

ForgeRock Stability Label Definitions

Stability Label	Definition
Stable	This documented feature or interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	This documented feature or interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release. While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.
Legacy	This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock. You should migrate to the newer version, however the existing functionality will remain. Legacy features or interfaces will be marked as *Deprecated* if they are scheduled to be removed from the product.

Stability Label	Definition
Deprecated	This feature or interface is deprecated and likely to be removed in a future release. For previously stable features or interfaces, the change was likely announced in a previous release. Deprecated features or interfaces will be removed from ForgeRock products.
Removed	This feature or interface was deprecated in a previous release and has now been removed from the product.
Technology Preview	Technology previews provide access to new features that are considered as new technology that is not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT. Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums. ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an "AS-IS" basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.
Internal/Undocumented	Internal and undocumented features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. Getting Support

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.

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.