FORGEROCK®

Release Notes
/ Web Agents 5.5

Latest update: 5.5.1.0

Copyright © 2011-2018 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 5.5, consider the following points:
>
> - Web Agents 5.5 only support AM 5.5 and later.
>
> - Web Agents 5.5 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.
>
> - 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.

1.1. New Minor Release

Web Agents 5.5.1.0

- ForgeRock periodically issues patch and minor releases with important fixes to improve the functionality, performance, and security of your web agent deployments. Web Agents 5.5.1.0 is the latest minor release, targeted for AM 6.5 deployments and can be downloaded from the *ForgeRock BackStage* website. To view the list of fixes in this release, see Web Agents 5.5.1.0.

1.2. New Features

Web Agents 5.5

Web Agents 5.5 is a minor release that includes new features, functional enhancements and fixes.

- **Agents Sharing Runtime Resources**

  In earlier versions of the Apache and NGINX Plus agent, each agent instance had its own runtime resources and shared memory.

  Apache (Unix) and NGINX Plus Web Agents 5.5 default to share agent runtime resources, installation files and shared memory among all the agent instances. For example, the `Agent_1` and `Agent_2` instances write the same session logs and audit files (even though each one write to their own file), use the same agent policy cache, and run a single set of worker processes and background tasks.

  To support this change, web agents now log system information in a different log file. For more information, see "Important Changes to Existing Functionality".

  Sharing runtime resources and shared memory is configurable, and you should take it into account when upgrading to Web Agents 5.5. For more information, see "Configuring Whether Unix Web Agents Should Share Runtime Resources and Shared Memory" in the *User Guide*.

- **Validation Option Added to the agentadmin Command**

  Web Agents 5.5 adds a new option, `--V`, to validate agent configurations. Use this option to troubleshoot agent configuration issues in your environment, or before opening a ticket with ForgeRock's Customer Support.

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

1.3. Major Improvements

Web Agents 5.5

- **Shared Memory Requirement Reduced**

  Web Agents 5.5 now require a minimum of 16 MB of shared memory for the session and policy cache and the various worker process and, additionally, 32 KB of shared memory for the logging system, down from 140 MB.

  For more information, see "Other Requirements".

- **Improved File Permission Management for Unix Agents**

  Earlier versions of the Unix agents created several runtime files and resources in such a way that they were always owned by the `root` user.

  Web Agents 5.5 ensure that runtime resources and files are always created by the user relevant to the agent. For example, all runtime resources created by the NGINX Plus agent belong to the user specified in the `User` directive in the NGINX Plus server configuration file.

Moreover, Web Agents 5.5 include a new environment variable, `AM_RESOURCE_PERMISSIONS`, which specifies the permissions that the agent sets for its runtime resources based on the value of `umask`.

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

- **REST Response Timeout Now Configurable**

You can now use the `com.sun.identity.agents.config.receive.timeout` property to configure the amount of time, in seconds, to wait for a response from the AM server.

The default is 4 seconds, which matches the previous hard-coded value.

For more information, see "Configuring Bootstrap Properties" in the *User Guide*.

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 Amazon Linux 2	6, 7	Apache HTTP Server 2.4 IBM HTTP Server 9.0 NGINX Plus R14, NGINX Plus R15
Microsoft Windows Server	2008 R2	Microsoft IIS 7.5 Apache HTTP Server 2.4[a]
	2012, 2012 R2	Microsoft IIS 8 Microsoft IIS 8.5 Apache HTTP Server 2.4[a]
	2016	Microsoft IIS 10 Apache HTTP Server 2.4[a]
Oracle Solaris x64 Oracle Solaris SPARC	10, 11	Apache HTTP Server 2.4
Ubuntu Linux	14.04 LTS 16.04 LTS 18.04 LTS	Apache HTTP Server 2.4 NGINX Plus R14 (*NGINX open source build 1.13.7*) NGINX Plus R15 (*NGINX open source build 1.13.10*)
IBM AIX	6, 7	IBM HTTP Server 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**
>
> 1. Web Agents 5.5 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 5.5 *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 the WebSocket protocol.

The following table summarizes OpenSSL support in Agents 5.5:

Supported OpenSSL Versions

Operating Systems	OpenSSL Versions
CentOS Red Hat Enterprise Linux Oracle Linux Ubuntu Linux	OpenSSL 1.0.x, OpenSSL 1.1.0, 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 web agents use the native Windows SSL libraries by default.

FORGEROCK

> **Note**
>
> OpenSSL 1.0.2 or newer 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.

2.4. 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*.

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 5.5.2.0

- 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 5.5.2.0 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.

Web Agents 5.5.1.0

- There are no important changes to existing functionality in this release.

Web Agents 5.5

- **Changes to the Logging System**

  Earlier versions of the web agents logged system information to the `/web_agents/`*`agent_type`*`/log/agent.log` file.

  Web Agents 5.5 log system information to the `/web_agents/`*`agent_type`*`/log/system_n.log`, where *n* indicates the agent group number.

  Consider an environment with two Apache server installations:

  - `Apache_1` has two agent instances configured, `agent_1` and `agent_2`, configured to share runtime resources (AmAgentId is set to 0). Both agent instances will write to the `syslog_0.log` file.

  - `Apache_2` has one agent instance configured, `agent_3`, with AmAgentId set to 1. The instance will write to the `syslog_1.log` file.

  The `system_n.log` file can contain the following information:

- Agent version information, written when the agent instance starts up.

- Logs for the agent background processes.

- Web Socket connection errors.

- Cache stats and removal of old POST data preservation files.

- Agent notifications.

Moreover, the `AM_DEFAULT_LOG_LEVEL` environment property has been renamed to `AM_SYSTEM_LOG_LEVEL`. Use this property to set up the log level for the instances. For more information, see Web Agent Environment Properties in the *User Guide*.

- **Changes to AM URL Validation**

  In earlier versions, web agents used the following properties to validate that it could reach the AM instances it was connected to:

  - `com.forgerock.agents.ext.url.validation.default.url.set`

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

  - `com.forgerock.agents.ext.url.validation.ping.interval`

  - `com.forgerock.agents.ext.url.validation.ping.miss.count`

  - `com.forgerock.agents.ext.url.validation.ping.ok.count`

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

  Web Agents 5.5 removes all the properties but `com.sun.identity.agents.config.naming.url` property, which should be configured to the load balancer in front of the AM instances (or load balancers, in case of having multiple sites).

- **Changes to agentadmin --v Command Output**

  Information regarding system resources is no longer included in the output from the **agentadmin --v** command.

  System resource information is now displayed by using the new **agentadmin --V** (Validator) command. For more information, see "Command-Line Tool Reference" in the *User Guide*

- Agents Timestamp Events in Coordinated Universal Time (UTC)

  When logging to a file, previous versions of the web agents timestamped events using the current timezone configured for the server.

  Web Agents 5.5 timestamp events in UTC.

3.2. Deprecated Functionality

Web Agents 5.5.1.0

• There is no deprecated functionality in this release.

Web Agents 5.5.0

• There is no deprecated functionality in this release.

3.3. Removed Functionality

Web Agents 5.5.1.0

• No components were removed in this release.

Web Agents 5.5

• `AM_DEFAULT_LOG_LEVEL` **Environment Property Renamed**

The `AM_DEFAULT_LOG_LEVEL` has been renamed to `AM_SYSTEM_LOG_LEVEL`.

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

• **Removed properties**

The following properties have been removed from Web Agents 5.5:

- `com.forgerock.agents.ext.url.validation.default.url.set`

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

- `com.forgerock.agents.ext.url.validation.ping.interval`

- `com.forgerock.agents.ext.url.validation.ping.miss.count`

- `com.forgerock.agents.ext.url.validation.ping.ok.count`

Chapter 4
Fixes, Limitations, and Known Issues

4.1. Key Fixes

Web Agents 5.5.1.0

- AMAGENTS-1933: init_ssl errors fill error_log

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

- AMAGENTS-1982: Custom login page issue when handling advices

- AMAGENTS-2053: Web agent does not honour com.sun.identity.agents.config.attribute.multi.value.separator value

- AMAGENTS-2085: Web Agent 5 should not have a value for com.sun.identity.client.notification.url property in OpenSSOAgentConfiguration.properties

- AMAGENTS-2095: Agent validator crash on Windows with erroneous agent.conf file

- AMAGENTS-2147: Agent 5.5x has a race condition creating semaphores on centos 32

- AMAGENTS-2150: Update pcre and http_parser libraries for agents 5.5.0.1

- AMAGENTS-2152: Original_request_url is not present after upgrading to Agent 5

- AMAGENTS-2153: WPA resource leak in json_find_node

Web Agents 5.5

- AMAGENTS-1840: Agent's version information disappear from the debug.log

- 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 auth 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

- AMAGENTS-1511: Agent5 is crashing on Apache for Windows server shutdown

- AMAGENTS-1510: Agent5 is crashing with unchecked use of r->conf->jwt_name value

- AMAGENTS-1509: Agent5 is crashing with unchecked use of r->conf->redirect_uri value

- AMAGENTS-1408: SIGSEGV when trying to install agent 5 with wrong AM version

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

4.2. Limitations

Web Agents 5.5.1.0

- There are no additional limitations and workarounds in this release. Refer to previous releases for more information.

Web Agents 5.5.0

The following limitations and workarounds apply to Web Agent 5.5:

- **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 5.5.1.0

- 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

Web Agents 5.5

- **CA Certificate File Name Property not Honored when Client Authentication is not Required in Secure Channel Environments**

  If you are using the Windows built-in Secure Channel API but your environment does not require client authentication, instead of setting the CA certificate friendly name in the CA Certificate File Name Property, set it in the Public Client Certificate File Name property. For example:

```
com.forgerock.agents.config.cert.ca.file =
com.forgerock.agents.config.cert.file = CA-cert-friendly-name
com.sun.identity.agents.config.trust.server.certs = false
```

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

  IIS web agents configured for client-based 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 anymore. 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 installations, and must be removed for IIS web agents configured for stateless (client-based) 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.

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

- AMAGENTS-1486: Agents 5 bootstrap retry settings are not used

- 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-1156: Disabled "Agent Configuration Change Notification" does not work properly, if new worker is created for C Agent

- 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-769: org.forgerock.agents.config.cdsso.deny.cleanup.disable property is not valid for C Agent 5

- AMAGENTS-704: C Agent 5 returns 403, if you don't login immediately

- 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

FORGEROCK

Chapter 5
Documentation Updates

The following table tracks changes to the documentation set following the release of AM Web Agent 5.5:

Documentation Change Log

Date	Description
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*.
2018-02-08	Release of Web Agents 5.5.2.0. • Updated the default value of `com.sun.identity.agents.config.fqdn.check.enable` to `false`. For more information, see Web Agents 5.5.2.0.
2018-12-05	Release of Web Agents 5.5.1.0.
2018-12-05	Updated the section to secure communications between AM and the agents to include information about AM 6.5 and later. For more information, see "Configuring Access Management Servers to Communicate With Web Agents" in the *User 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 "Configuring Bootstrap Properties" in the *User Guide*.
2018-09-19	First release of Web Agents 5.5

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.