Release Notes

/ ForgeRock Access Management 5.5

Latest update: 5.5.2

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

Abstract

Notes covering new features, fixes and known issues in ForgeRock® Access Management. ForgeRock Access Management provides authentication, authorization, entitlement, and federation software.

Table of Contents

Preface

Read these release notes before you install ForgeRock Access Management or update your existing installation.

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

This chapter covers the new features and improvements done in the current release of ForgeRock Access Management.

1.1. 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.

AM 5.5.2

- AM 5.5.2 is the latest release targeted for AM 5.5 deployments and can be downloaded from the *ForgeRock Backstage* website. To view the list of fixes in this release, see Key Fixes in AM 5.5.2.

  The release can be deployed as an initial deployment or updated from an existing 5.5 or 5.5.1 deployment, see "Supported Upgrade Paths". AM 5.5 and AM 5.5.1 are available for download at the *ForgeRock Backstage* website: *5.5*, *5.5.1*.

1.2. New Features

New Features in AM 5.5.2

AM 5.5.2 introduces the following:

- Added Support for Affinity-based Deployments of ForgeRock Directory Services Identity Stores

  AM 5.5.2 adds support for identity stores to configured as an affinity deployment, in the same way as CTS, application, and policy stores.

  Specify each of the directory server instances that form the affinity deployment in the LDAP Server field, when configuring identity stores.

  In an affinity-based deployment, the Directory Services instance used for each operation is based on the DN of the identity involved.

For more information, see "Directory Services Configuration Properties" in the *Setup and Maintenance Guide*.

- **Many Other Improvements**. See Improvements in AM 5.5.2.

New Features in AM 5.5.1

ForgeRock Access Management is a maintenance release that includes a new endpoint version and one fix.

- **New `/sessions` Endpoint Version**

  The `/sessions` endpoint has a new API version, `v3.0`, which stores the session token ID in the POST body as a JSON object.

  New endpoint versions may modify the endpoint's default API version. To avoid version conflicts between application calls and REST endpoint APIs, consider specifying the protocol and resource version required by the application in the `Accept-API-Version` header when making requests to REST endpoints. For more information, see "Review REST API Versions Before Upgrading" in the *Upgrade Guide*.

  For more information about the `/sessions` `v3.0` endpoint, see AM's API explorer.

New Features in AM 5.5.0

ForgeRock Access Management 5.5.0 is a major release that introduces new features, functional enhancements, and fixes.

-

  Authorization

  - **Transactional Authorization**

    AM 5.5.0 includes a new transaction-based policy condition. Access to a resource or API can now require interactive user confirmation, for example responding to a push notification in the ForgeRock Authenticator app or confirmation of a one-time password sent by email.

    Each transactional authorization provides a single access to the protected resource, protecting against replay attacks.

    If you use transactional authorization alongside web or Java agents, they must be at least version 5.

    For more information, see "*Implementing Transactional Authorization*" in the *Authorization Guide*.

- *Authentication*

  - **Fine-Grained Authentication**

    Earlier versions of AM provided authentication chains to configure different authentication modules together. AM 5.5.0 adds the concept of authentication trees, which provide fine-grained authentication by allowing multiple paths and decision points throughout the authentication flow.

    For more information, see "About Authentication Trees" in the *Authentication and Single Sign-On Guide*.

  - **New Social Authentication Modules**

    AM 5.5.0 includes new authentication modules for authenticating Instagram, VKontakte, and WeChat users.

    New generic OAuth 2.0 and OpenID Connect 1.0 authentication modules are also included.

    For more information, see "Social Authentication Modules" in the *Authentication and Single Sign-On Guide*.

  - **New IDM User Self Registration Service**

    You can configure IDM as a provisioning service in AM. This allows IDM to complete user registration after authenticating to AM using a social identity provider authentication module.

    For more information, see "Configuring User Registration" in the *User Self Service Guide*.

- *OAuth 2.0 Applications*

  - **OAuth 2.0 Dynamic Client Registration Support**

    AM 5.5.0 adds support for the *OAuth 2.0 Dynamic Client Registration Protocol*, which allows OAuth 2.0 client applications to register dynamically with AM as an authorization server.

    AM supports open registration, registration with an access token, and registration including a secure software statement issued by a software publisher. For details and examples, see "To Configure AM for OAuth 2.0 Dynamic Client Registration" in the *OAuth 2.0 Guide*.

  - **OAuth 2.0 Remote Consent Service Support**

    AM 5.5.0 adds AM support for remote OAuth 2.0 consent services, which allow the consent-gathering part of an OAuth 2.0 flow to be handed off to a separate service.

    The remote consent service renders the consent page, gathers the result, signs and encrypts the result, and returns it to the authorization server.

For details and examples, see "OAuth 2.0 Remote Consent Service" in the *OAuth 2.0 Guide*.

- **New OAuth 2.0 Stateless Access Token Claims**

  AM 5.5.0 adds new OAuth 2.0 stateless access token claims, `"grant_type"`, `"auth_level"`, and `"auth_time"`.

  - **"grant_type"**. The `"grant_type"` claim indicates the type of authorization flow that the user has completed. This information is useful for the resource server to make decisions based upon both the scopes and the grant type of the user.
  - **"auth_level"**. The `"auth_level"` claim enables the authentication level to persist beyond the lifetime of the original authentication flow.
  - **"auth_time"**. The `"auth_time"` claim indicates the original authentication time in seconds.

- *Privacy and Consent*

  - **User Managed Access (UMA) 2.0**

    AM 5.5.0 supports the architecturally-simplified UMA 2.0 protocol, which provides the following capabilities:

    - Enhanced user control over their data
    - Support for UMA 2.0 grant for OAuth2 authorization flow
    - Support for UMA 2.0 federated authorization

    UMA 1.0.x is no longer supported.

    For more information, see "*Introducing UMA 2.0*" in the *User-Managed Access (UMA) 2.0 Guide*.

- *General*

  - **Added Support for Amazon Linux AMI 2017.03**

    AM now can be installed on Amazon Linux AMI 2017.03. For more information, see "Operating System Requirements".

  - **Added Support for Oracle Unified Directory 11g R2**

    Oracle Unified Directory 11g R2 can now be used as a user data store. For more information, see "Data Store Requirements".

  - **Amster 5.5.0 Released**

Amster 5.5.0 allows you to export and import configurations for AM 5.5.0 and later. For more information, see the *ForgeRock Amster Release Notes*.

1.3. Major Improvements

Improvements in AM 5.5.2

- OPENAM-6426: Forgot password should print an audit log
- OPENAM-6748: Improve mechanics of the notification cache
- OPENAM-9674: Support Active Directory Recursive Group Membership Lookup
- OPENAM-11312: Attribute Mapping defined in wsfed remote SP should not be overridden by attribute mapping defined in wsfed OpenAM Hosted IDP
- OPENAM-12140: Allow USS Registration route to be configurable
- OPENAM-12184: Extend the DJ/DS SDK affinity LB feature to the userstore connection
- OPENAM-12255: Process SMS notifications sequentially by default instead of using a threadpool
- OPENAM-12261: Honor org.apache.xml.security.ignoreLineBreaks=true when generating WS-Fed Assertions
- OPENAM-12965: httpClient not exposed to OIDC Claim Script
- OPENAM-13088: RFE: add option for isInitiator=false to WDSSO configuration
- OPENAM-13330: Improve SessionReource Authz Module processing
- OPENAM-13838: Wording on "Maximum Caching Time" requires an update
- OPENAM-14939: Enable "org.apache.xml.security.ignoreLineBreaks=true" by default
- OPENAM-14940: Improve SAML2 Response/Assertion generation to not have carriage return inbetween XML tag
- OPENAM-15899: Have an option to add <ds:X509Certificate> tag in the signed SLO request

Improvements in AM 5.5.1

- There are no major improvements or enhancements in this release, only bug fixes.

Improvements in AM 5.5.0

- **Merged Debug Log Messages to Standard Output**

AM now reads a Java system property to determine whether to write debug messages to files in the `debug` directory or to standard output.

For details, see "Debug Logging to a Single File or to Standard Output" in the *Setup and Maintenance Guide*.

- **Reduced Metadata for Stateless OAuth 2.0 Tokens**

  AM now stores less metadata in the CTS when the server uses stateless OAuth 2.0 tokens. This improvement does not render any existing OAuth 2.0 tokens invalid.

  When you upgrade an AM server, the upgrade process enables stateless grant token upgrade compatibility mode. This mode allows the CTS to store both former and current formats of Stateless OAuth 2.0 token metadata. The mode enables you to benefit from the improvement when performing a rolling, zero-downtime upgrade of an AM cluster.

  After successfully upgrading all servers in the cluster, disable this mode on each AM server in one of the following ways:

  - In the AM console, under Configure > Global Services > OAuth2 Provider, disable stateless grant token upgrade compatibility mode, and save the change.
  - Set the global OAuth2 Provider service property, `statelessGrantTokenUpgradeCompatibilityMode`, to `false`.

- **Improved Cross-Domain Single Sign-On Capabilities**

  Starting with Web Agents 5 and Java Agents 5, CDSSO capabilities have been enhanced:

  - CDSSO now provides SSO capabilities for AM and web or Java agents in a single DNS domain and cross-domains, which simplifies SSO configuration. For more information, see "About Single Sign-On" in the *Authentication and Single Sign-On Guide*.
  - CDSSO now supports stateless sessions, with the following caveats:
    - Stateless sessions do not support restricted tokens. Therefore, web or Java agents 5 configured in a stateless realm are not protected against cookie hijacking. ForgeRock recommends using web or Java agents with stateful sessions.
    - To ensure the stateless session cookie size does not surpass the browser supported size, Web Agents 5 and Java Agents 5 does not support both signing and encrypting the stateless session cookie.

  For more information, see "Cross-Domain SSO" in the *Authentication and Single Sign-On Guide* and "Configuring Stateless Session Cookie Security" in the *Authentication and Single Sign-On Guide*.

CDSSO capabilities for web or Java agents earlier than version 5 are still supported, but have been renamed to classic CDSSO. For more information, see "Implementing Classic Single Domain and Cross-Domain SSO" in the *Authentication and Single Sign-On Guide*.

- **Authentication Level and OAuth 2.0 Access Tokens**

  Before a resource owner grants consent to an OAuth 2.0 client, the resource owner authenticates with AM. Upon successful authentication AM assigns an authentication level as described in "About Authentication Levels" in the *Authentication and Single Sign-On Guide*.

  AM now associates the authentication level with the access tokens that it issues to the OAuth 2.0 client. When a client introspects the access token, AM returns the authentication level as the value of an `auth_level` claim in the response. An example claim is shown in the /oauth2/introspect example in "OAuth 2.0 Client and Resource Server Endpoints" in the *OAuth 2.0 Guide*.

  This claim is added automatically, with no configuration required to enable it. It is available for all OAuth 2.0 flows, except the client credential flow.

1.4. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

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

Chapter 2

Before You Install

This chapter covers software and hardware prerequisites for installing and running ForgeRock Access Management server 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. Files to Download

AM software is available at https://backstage.forgerock.com. For a description of the files available for download, see "AM Software".

AM Software

File	Description
`AM-5.5.2.zip`	Cross-platform distribution including all software components. For a list of the files in the .zip archive, see "Obtaining Software" in the *Installation Guide*.
`AM-5.5.2.war`	Deployable web application archive file.
`SSOAdminTools-5.1.1.8.zip`	The .zip file that contains tools to manage AM from the command line.
`SSOConfiguratorTools-5.1.1.8.zip`	The .zip file that contains tools to configure AM from the command line.

2.2. Operating System Requirements

ForgeRock supports customers using ForgeRock Access Management server software on the following operating system versions:

Supported Operating Systems

Operating System	Version
Red Hat Enterprise Linux, Centos, Amazon Linux	6, 7
Amazon Linux	Amazon Linux AMI 2017.03
SuSE	11
Ubuntu	14.04 LTS, 16.04 LTS
Solaris x64	10, 11
Solaris Sparc	10, 11
Windows Server	2012, 2012 R2, 2016

2.3. Java Requirements

JDK Requirements

Vendor	Version
Oracle JDK	8
IBM SDK, Java Technology Edition (Websphere only)	8
OpenJDK	8

2.4. Web Application Container Requirements

The following table summarizes supported application containers and their required versions:

Web Containers

Web Container	Versions
Apache Tomcat	7[a], 8.5, 9
Oracle WebLogic Server	12c
JBoss Enterprise Application Platform	7.0
WildFly AS	9, 10, 10.1
IBM WebSphere	8.5.5.8+

[a] We recommend that you not use Apache Tomcat version 7.0.15+. We have found a bug where Tomcat throws a SocketTimeoutException when the application tries to read the request InputStream under high load. This issue affects Apache Tomcat 7.0.15+ and was fixed in version 8.5. For more information, see https://github.com/apache/tomcat80/pull/9.

The web application container must be able to write to its own home directory, where AM stores configuration files.

Caution

Java Agents and Web Agents 5 and later require the WebSocket protocol to communicate with AM.

Ensure that the container where AM runs, the web server/container where the agents run, and your network infrastructure all support the WebSocket protocol.

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

2.5. Data Store Requirements

This section lists supported data stores.

As described in "Generic LDAPv3 Configuration Properties" in the *Setup and Maintenance Guide*, you can configure AM to use LDAPv3-compliant directory servers as user data stores. If you have a special request to deploy AM with a user data store not mentioned in the following table, contact info@forgerock.com.

Supported Data Stores

Data Store	Version	CTS Datastore	Config Datastore	User Datastore	UMA Datastore
Embedded Directory Services	5.5.3	✔	✔	✔	✔
External Directory Services/ OpenDJ	3.0+	✔	✔	✔	✔
Oracle Unified Directory	11g R2			✔	
Oracle Directory Server Enterprise Edition	11g			✔	
Microsoft Active Directory	2012, 2012 R2, 2016			✔	
IBM Tivoli Directory Server	6.3			✔	

2.6. Supported Clients

The following table summarizes supported clients and their minimum required versions:

Supported Clients

Client Platform	Native Apps [a]	Chrome 62.0.3202[b]	Internet Explorer 11+	Edge 25.10586	Firefox 57+[b]	Safari 11[b]	Mobile Safari
Windows 8	✔	✔	✔		✔		
Windows 10	✔	✔	✔	✔	✔		
Mac OS X 10.11 or later	✔	✔			✔	✔	
Ubuntu 14.04 LTS or later	✔	✔			✔		
iOS 9 or later	✔	✔					✔
Android 6 or later	✔	✔					

[a] *Native Apps* is a placeholder to indicate AM is not just a browser-based technology product. An example of a native app would be something written to use our REST APIs, such as the sample OAuth 2.0 Token Demo app.

[b]Chrome, Firefox, and Safari are configured to update automatically, so customers will typically be running latest. However, for RFP reasons, we specify a minimum version.

2.7. Supported Upgrade Paths

The following table contains information about the supported upgrade paths to AM 5.5.2:

Upgrade Paths

Version	Upgrade Supported?
AM 5.x	✔ [a]
OpenAM 13.x.x	✔

a

[a]**Caution**
Access Management is incompatible with SSO session tokens from OpenAM.
Storage and processing of SSO tokens changed in AM 5, meaning both stateful and stateless SSO sessions created in earlier versions of OpenAM are not supported.
After upgrading from an earlier version, any existing SSO tokens created by that version will become invalid, and users will need to reauthenticate.
In mixed version deployments, earlier versions of OpenAM will not be able to read or process SSO session tokens created by AM 5 or later.

This incompatibility only affects SSO session tokens. OAuth 2.0 and OpenID Connect 1.0 tokens are interoperable between versions.

Note

Upgrading between Enterprise and OEM versions is not supported.

For more information, see Checking your product versions are supported in the *ForgeRock Knowledge Base*.

2.8. Special Requests

If you have a special request regarding support for a combination not listed here, contact ForgeRock at info@forgerock.com.

Chapter 3
Installing or Upgrading

This chapter covers installing and upgrading AM 5.5 software.

Before you install AM or upgrade your existing installation, read these release notes. Then, install or upgrade AM.

Warning

For web containers, if you plan to use Apache Tomcat with AM 5.5.0, we recommend using Apache Tomcat 8.5. We have found a bug where Tomcat throws a SocketTimeoutException when the application tries to read the request InputStream under high load. This affects Apache Tomcat 7.x.15+ and all of 8.0.x; therefore, we highly recommend the use of Tomcat 8.5, where the bug appears to be fixed. For more information, see https://github.com/apache/tomcat80/pull/9.

- If you are installing AM for the first time, see the Installation Guide.
- If you have already installed AM, see the Upgrade Guide.

  Do *not* perform an upgrade by deploying the new version and then importing an existing configuration by running the **ssoadm import-svc-config** command. Importing an outdated configuration can result in a corrupted installation.

Chapter 4

Changes and Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

4.1. Important Changes to Existing Functionality

This section lists changes done to existing functionality, services, endpoints, and others in the current release of AM.

Caution

Access Management is incompatible with SSO session tokens from OpenAM.

Storage and processing of SSO tokens changed in AM 5, meaning both stateful and stateless SSO sessions created in earlier versions of OpenAM are not supported.

After upgrading from an earlier version, any existing SSO tokens created by that version will become invalid, and users will need to reauthenticate.

In mixed version deployments, earlier versions of OpenAM will not be able to read or process SSO session tokens created by AM 5 or later.

This incompatibility only affects SSO session tokens. OAuth 2.0 and OpenID Connect 1.0 tokens are interoperable between versions.

Important Changes in AM 5.5.2

- OPENAM-15444: Prepare for Chrome's move to SameSite=lax by default
- OPENAM-15841: DisableSameSiteCookiesFilter broken on WebLogic

  These fixes add a new filter that sets the `SameSite=None` attribute for all secure AM cookies on compatible browsers. For more information on the SameSite cookie support, see the *ForgeRock Knowledge Base* website.
- Many other improvements were introduced in this release. See Improvements in AM 5.5.2.

Important Changes in AM 5.5.1

- LDAPv3Repos LDAP Servers are Now Stored as Comma-Separated Ordered Lists

For multiple data stores behind a load balancer deployment, AM now stores its servers as a comma-separated list, rather than orderedlist.

For example, given a site configuration, ID 02, with two servers, IDs 01 and 03. In previous releases (prior to AM ${am.software.version} and earlier), AM would store the servers as an orderedlist:

```
$./ldapsearch -p 51389 -D "cn=Directory Manager" -w cangetin -b "ou=services,dc=openam,dc=forgerock
,dc=org" "objectclass=*"  > backup.ldif
$ grep "sun-idrepo-ldapv3-config-ldap-server" backup.ldif
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=xxx.example.com:1389|01|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1389|01|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=xxx.example.com:1389|03|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=localhost:51389
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1389|03|02
```

Now, AM stores its multi-server configuration as a comma-separated ordered list:

```
$./ldapsearch -p 51389 -D "cn=Directory Manager" -w cangetin -b "ou=services,dc=openam,dc=forgerock
,dc=org" "objectclass=*"  > backup.ldif
   $ grep "sun-idrepo-ldapv3-config-ldap-server" backup.ldif
   sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=[0]=xxx.example.com:1389|01|02,xxx.example
.com:1389|03|02,localhost:51389,zzz.example.com:1389|01|02,zzz.example.com:1389|03|02
```

Important Changes in AM 5.5.0

- **Removed Support for UMA 1.0**

  AM no longer supports UMA 1.0 and now supports UMA 2.0.

- **Do Not Enable org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH in Production**

  It is strongly recommended *not* to use the forward slash character in policy names. Users running AM servers on Tomcat and JBoss web containers will not be able to manipulate policies with the forward slash character in their names without setting the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` argument in the `CATALINA_OPTS` environment variable before starting the AM web container.

  It is also strongly recommended not to enable the `org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting while running AM in production. Using this option introduces a security risk. See Apache Tomcat 6.x Vulnerabilities and the related CVE for more information.

  If you have policy names with forward slashes after migration to AM 5.x, rename the policies so that they do not have forward slashes. Perform the following steps if you use Tomcat or JBoss as your AM web container:

  1. Stop the AM web container.
  2. Add the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting to the `CATALINA_OPTS` environment variable.
  3. Restart the AM web container.

4. Rename any policies with forward slashes in their names.
5. Stop the AM web container.
6. Remove the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting from the `CATALINA_OPTS` environment variable.
7. Restart the AM web container.

- **Simplified Deployment of Custom Authentication Modules**

  AM 5.5.0 no longer requires registration of custom modules using the **ssoadm** command. Instead, it uses a service loader to register custom modules' service schemas.

  Make the following changes when deploying a custom authentication module in AM 5.5.0:

  - Include a class in the custom authentication module's `.jar` file that invokes the service loader to register the custom module's service schema.

    For an example class, see the `SampleAuthPlugin.java` file in the custom authentication module sample.

  - Include the `META-INF/services/org.forgerock.openam.plugins.AmPlugin` resource file in the custom authentication module's `.jar` file. This resource file holds the fully qualified name of the class that registers the custom implementation.

    For an example resource file, see the `org.forgerock.openam.plugins.AmPlugin` file in the custom authentication module sample.

  - Update the script or Maven `pom.xml` file that you use when you build the custom authentication module. Note that the build dependencies have changed since version 5.0 of AM, so you will probably need to change your script or `pom.xml` file. For an example of a `pom.xml` file that you can use to build a custom authentication module with a service loader, see the custom authentication module sample.

  - After you have changed your build script or Maven `pom.xml` file, rebuild the custom authentication module.

  - Do *not* register custom modules referred to in the `SampleAuthPlugin.java` and `AmPlugin` files with the **ssoadm** command, as was required in earlier versions of AM.

  For detailed information about the custom authentication module sample, see "Creating a Custom Authentication Module" in the *Authentication and Single Sign-On Guide*.

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

  Java Agents 5 and Web Agents 5 do not support policies configured with the Identity Membership(`AMIdentityMembership`) environment condition. Instead, configure the equivalent User & Group (`Identity`) subject condition.

- **Change to Client Credentials for Dynamic OpenID Connect Registration**

  When you register an OpenID Connect client dynamically, AM generates `client_id` and `client_secret` values. AM now ignores any values provided in the client metadata for these properties.

- **Removed JWT as OAuth 2.0 Grant Type**

  `JWT` is no longer an authorization grant bearer type for OAuth 2.0. For more information, see "JWT Bearer Profile" in the *OAuth 2.0 Guide*.

- **Changes in the OpenID Connect Client Registration Endpoint**

  Due to the implementation of the OAuth2 Dynamic Client Registration specification (RFC7591), the OpenID Connect (OIDC) client registration endpoint (`/oauth2/connect/register`) has seen the following changes:

  - Using the `scopes` parameters in the payload is deprecated in favor of the `scope` parameter.
  - The `/oauth2/connect/register` endpoint is deprecated in favor of the `/oauth2/register` endpoint.

    The `/oauth2/register` endpoint does not default to include the `openid` scope. Therefore, when registering OpenID Connect clients using REST or the AM console, you must specify the `openid` scope.

    The deprecated `/oauth2/connect/register` endpoint included the `openid` scope by default.
  - If the `client_id` and the `client_secret` values are specified in the registration request payload, AM ignores them and uses server-generated values in their place.

    Previously, these fields could be provided by the client in the registration request payload.

- Removed Microsoft Live Social Authentication Wizard

  The wizard for configuring Microsoft Live as a social authentication providers has been removed in AM 5.5.0.

  To configure Microsoft Live as a social authentication provider, manually configure the following:

  - The OAuth 2.0 Provider service
  - The Social Authentication Implementation service
  - An OAuth 2.0 social authentication module
  - An authentication chain containing the module

  For more information on configuring these components, see "*Implementing Social Authentication*" in the *Authentication and Single Sign-On Guide*.

4.2. Deprecated Functionality

Functionality listed under this section has been deprecated and will be removed in a future release of AM.

Deprecated in AM 5.5.2

- No features have been deprecated in this release.

Deprecated in AM 5.5.1

- No features have been deprecated in this release.

Deprecated in AM 5.5.0

- OAuth 2.0 / OpenID Connect Authentication Module Deprecated

  The combined OAuth 2.0 / OpenID Connect authentication module is deprecated in this release.

  AM 5.5.0 provides replacement individual authentication modules. See "Social Authentication Modules" in the *Authentication and Single Sign-On Guide*.

- **amverifyarchive Tool Deprecated**

  The **amverifyarchive** tool will be removed in a future release of ForgeRock Access Management.

- `/oauth2/connect/register` **Endpoint Deprecated**

  The `/oauth2/connect/register` endpoint has been deprecated. Use the `/oauth2/register` endpoint instead.

- **Use of Realm Paths to Specify Realm in REST Requests is Deprecated**

  Using a realm path in the URL of a REST request as follows is now deprecated:

  ```
  $ curl 'https://openam.example.com:8443/openam/json/subrealmA/subrealmB/users/demo'
  ```

  This method for specifying realms is deprecated and will be removed in a future version.

  You must instead prefix each realm in the tree hierarchy with the `realms` keyword, and explicitly include the `root` realm, as follows:

  ```
  $ curl 'https://openam.example.com:8443/openam/json/realms/root/realms/subrealmA/realms/subrealmB/users/
  demo'
  ```

  Important

  This change applies to the following REST endpoint paths:

  - `/json/*`

- `/oauth2/*`
- `/uma/*`

For more information on specifying realms in REST API URLs, see "Specifying Realms in REST API Calls" in the *Authentication and Single Sign-On Guide*.

4.3. Removed Functionality

Functionality listed under this section has been removed from AM.

Removed in AM 5.5.2

- No features have been removed in this release.

Removed in AM 5.5.1

- No features have been removed in this release.

Removed in AM 5.5.0

- **Removal of JWT as Authorization Grant Bearer Type**

  AM has removed support for the JWT authorization grant bearer type as specified in Section 2.1 of RFC 7523, *Using JWTs as Authorization Grants*.

  AM continues to support Section 2.2, *Using JWTs for Client Authentication*, of RFC 7523. For more information, see "JWT Bearer Profile" in the *OAuth 2.0 Guide*.

- **Removal of Crosstalk-related Properties**

  The following system configuration properties have been removed from AM:

  - com.iplanet.am.session.failover.cluster.stateCheck.period
  - com.iplanet.am.session.failover.cluster.stateCheck.timeout

- **Removal of UrlAccessAgent**

  The `UrlAccessAgent` user has been removed from AM and Amster.

- **Removal of AM SDK**

  The AM SDK has been removed. This includes the Java `com.iplanet.am.sdk` package, which has been deprecated since Sun Java System Access Manager 7.1. The client detection service has also been removed.

When you upgrade AM software, the following settings are removed:

- Settings for running in coexistence mode with Sun Access Manager
- `com.iplanet.am.domaincomponent` property settings
- `com.iplanet.am.sdk.ldap.debugFileName` property settings
- `com.iplanet.am.sdk.userEntryProcessingImpl` property settings
- `com.sun.identity.amsdk.cache.enabled` property settings

- **Removed Client SDK Software**

  Deprecated client SDK examples and libraries have been removed.

  Client applications can use the AM REST APIs instead, as documented in "*Developing with the REST API*" in the *Development Guide*.

- **Removed Support for JDK 7**

  AM 5.5.0 supports JDK 8 only. For more information, see "Java Requirements".

- **Removed Support for Several Data Store Versions**

  AM 5.5.0 does not support the following data store versions:

  - OpenDJ 2.6.x
  - Oracle Unified Directory 11g

  For more information, see "Data Store Requirements".

- **Removed Support for Amazon Linux 2016.09**

  AM now supports Amazon Linux AMI 2017.03. For more information, see "Operating System Requirements".

- **Removed the `ssoadm.jsp` Page**

  The deprecated `ssoadm.jsp` page has been removed.

- **Removed the Default Agent, `UrlAccessAgent`**

  The default agent, `UrlAccessAgent`, has been removed. Therefore, you need only to provide the `amAdmin` user password during AM installation.

  The `--PolicyAgentPwd` option has also been removed from the **ssoadm** command.

Chapter 5

Fixes, Limitations, and Known Issues

This chapter covers the status of key issues and limitations at release 5.5.

5.1. Key Fixes

Key Fixes in AM 5.5.2

- OPENAM-1167: WindowsDesktopSSOConfig ClassCastException on saving configuration in admin UI
- OPENAM-4040: SSO failure between SPs in separate CoTs with same hosted IDP
- OPENAM-5865: AuthLevelCondition will not retrieve request auth level for a capital-letter realm.
- OPENAM-5867: Data Store LDAP server (admin-ordered) list is reordered by OpenAM
- OPENAM-6141: REST-SMS: Request for sts and dashboard services schema returns 500
- OPENAM-6370: REST-SMS: 500 Internal Server Error for Invalid Attribute Update
- OPENAM-6426: Forgot password doesn't print an audit log
- OPENAM-6445: UMA policy with self-sharing creating policy despite failure
- OPENAM-6748: Improve mechanics of the notification cache
- OPENAM-6925: When getting a access token with a Basic HTTP client and a invalid grant_type the wrong error is returned
- OPENAM-8264: Insufficient validator for service property 'iplanet-am-auth-hmac-signing-shared-secret'
- OPENAM-9674: Support Active Directory Recursive Group Membership Lookup
- OPENAM-9783: json/users changePassword returns the wrong error message with multiple datastores
- OPENAM-9790: Allow IDP to determine request binding from goto url as well as request method
- OPENAM-9931: Global Session Service - two fields with the exact same name (Redundant 'Global Attributes' setting should be removed)

- OPENAM-10083: Sending READ to sites endpoint sometimes returns 500 error
- OPENAM-10191: Add Skew to NotOnOrAfter and NotBefore Assertion Conditions
- OPENAM-10296: Session UI only allows searching for users in datastore
- OPENAM-10371: NPE for notifyGlobalConfigChange in Configuration debug file after OpenAM setup
- OPENAM-10532: SOAPExceptionImpl: Invalid Content-Type:text/html. Is this an error message instead of a SOAP response?
- OPENAM-10591: Generate more debug details about the JSON that is failing when JsonPolicyParser throws a UNABLE_TO_SERIALIZE_OBJECT exception
- OPENAM-10619: Post Authentication Plugin not run during session upgrade
- OPENAM-10673: SAML2 authentication module fails to redirect to IDP after failing DeviceID match module
- OPENAM-10934: Authentication succeeds although DeviceIDSave module fails
- OPENAM-10935: DeviceIDSave - stacktrace is lost
- OPENAM-10994: Performance degradation of around 30% using defaults JCEKS so as to JKS
- OPENAM-11048: OpenAM account lockout does not work when naming attribute and LDAP Users Search Attribute are different
- OPENAM-11055: ssoadm command "set-attr-defs" reports success but does not actually update global service
- OPENAM-11087: Global Config Email Service SSL State has changed from SSL to non-SSL between versions 13.5.0 and 14.0.0
- OPENAM-11118: REST call allows for realm name with space when creating realm
- OPENAM-11157: Oauth2/OIDC Authentication redirect goto value wrong when behind reverse proxy
- OPENAM-11159: OpenAM Amster export/import for Site have import errors
- OPENAM-11167: <ActualLockoutDuration> is not updated in the attribute sunStoreInvalidAttemptsData
- OPENAM-11177: Scripted auth module can not be used in auth chain if the username in sharedstate map does not 'match' the search attribute of the data store
- OPENAM-11225: idpSingleLogoutRedirect throws 500 error SLO
- OPENAM-11240: "Skip This Step" button on the ForgeRock Authenticator (OATH) screen is missing (HOTP)

- OPENAM-11289: SP initiated SLO with SOAP binding fails with code 400
- OPENAM-11312: Attribute Mapping defined in wsfed remote SP should not be overridden by attribute mapping defined in wsfed OpenAM Hosted IDP
- OPENAM-11398: OpenAM ACI installation instruction does not work for OpenDJ productionMode
- OPENAM-11402: OpenAM does not enforce OAuth2 spec for "Resource Owner Password Credentials Grant" flow
- OPENAM-11407: Extra space in the CTS 's connection string " openam.internal.example.com:50389" cause OpenDJ-SDK log to grow
- OPENAM-11432: Extra space in Policy 's Resource Type will cause policy evaluation to fails
- OPENAM-11473: NumberFormatException on startup for External configuration setup
- OPENAM-11491: Upgrading OpenAM results in failure due to restSMS.xml
- OPENAM-11523: Using the LDAP/AD auth module, the change password on next login, if current password is empty it displays the wrong error message
- OPENAM-11547: Missing entry or corrupted value in "com.iplanet.am.version" causes upgrade failure
- OPENAM-11548: Improve Scope validator class loading error handling
- OPENAM-11565: Implicit grant flow is not generating an Ops token
- OPENAM-11619: Default scope value is incorrect (empty) for Social Auth VKontakte module
- OPENAM-11642: CustomProperties do not work when creating J2EE/Web Agents via REST
- OPENAM-11665: Improve debug logging when unable to login in XUI with users endpoint getting 404 due to KBA attribute issues
- OPENAM-11673: Policy evaluation response is incorrect if the URL query string sent for evaluation contains the string ://
- OPENAM-11678: 'Oldest' REST passwordreset selfservice unusable
- OPENAM-11746: Syslog data is not fully RFC compliant
- OPENAM-11789: User remains on 'Loading' page with 'OAuth2.0/OIDC' auth module if authId token expires before entering credentials
- OPENAM-11818: Oauth2 authn module incorrectly POST state parameter to token endpoint
- OPENAM-11829: SSOToken idletime reset even when it shouldn't be
- OPENAM-11863: CORSFilter position in web.xml should come before most filters

- OPENAM-11876: Amster has a timeout limit of 10 second and it is not configurable
- OPENAM-11909: Demo user creation is based on whether a userCfg is specified, rather than when it's set to embedded
- OPENAM-11925: CORSFIlter causing failures after moving to 5.x from 13.5.x
- OPENAM-11935: redirect_uri should be required in the OAuth2 authorization request
- OPENAM-11937: Federation UI does not allow empty NameIDMappingService
- OPENAM-11944: REST OAuth2 creation triggers objectClass=* search
- OPENAM-11956: SAML2 RelayState values are seen as invalid if they are not a URL which appears to go against the spec
- OPENAM-11961: KBA update fails if Self service is configured in sub-realm and root realm has no datastore
- OPENAM-11962: Calling Logout and passing a goto URL parameter with an expired session, goto URL is ignored
- OPENAM-11966: SAML2 SSO 'better' auth'n comparison fails with 'Invalid status code in response'
- OPENAM-11968: SAML2 Auth Module does not accept SAML2 AuthResponse with no SessionIndex
- OPENAM-11976: XUI Session query session by username does not work with +
- OPENAM-11980: Social OIDC wizards do not work when provisioning accounts locally
- OPENAM-11994: NullPointerException in ResourceOwnerOrSuperUserAuthzModule.getUserIdFromUri
- OPENAM-12022: Self-service registration for existing user displays "Detected conflict in request"
- OPENAM-12026: Self-service user registration gets "Bad Request" on LDAP error 19
- OPENAM-12037: Memory leak: LDAPFilterCondition creates new ShutdownManager listener on each request
- OPENAM-12054: Cumulative upgrades of OpenAM (e.g. 5.1.0 to 5.5.0 to 5.5.1) fail with "Writing Backup; Failed!" error
- OPENAM-12062: XUI DashBoard does not show trusted devices etc if user search attribute of the data store is not 'uid'
- OPENAM-12069: Non amadmin admin user can't edit Policy Sets / Policies
- OPENAM-12071: Error during upgrade with unindex search from UpgradeUtils.deleteService()
- OPENAM-12075: OIDC without a datastore returns "User must be authenticated to issue ID tokens"
- OPENAM-12078: OAuth 2 device flow loses OIDC nonce

- OPENAM-12079: Cannot use prompt=login with device flow
- OPENAM-12080: OAuth2 Stateless Session Signing Key lost during upgrade
- OPENAM-12082: Outlook with WS-Fed uses cached credential after AD password change.
- OPENAM-12098: Default server property com.sun.identity.urlchecker.dorequest is invalid
- OPENAM-12109: Syslog Audit Event Handler buffer size should be configurable
- OPENAM-12140: Allow USS Registration route to be configurable
- OPENAM-12144: getSessionInfo endpoint _fields parameter doesn't work
- OPENAM-12155: Client authenticate JWT with no exp and audience throw a NPE
- OPENAM-12161: Expires attribute in WS-Fed Active Requestor Profile is expected but is optional
- OPENAM-12166: Resource #3.0 logoutByHandle request fail with status 500 error
- OPENAM-12169: REST SMS deadlocks when processing notifications
- OPENAM-12170: NPE in PolicyConfig
- OPENAM-12171: PolicySetCache gets corrupted when the realm name contains upper case characters
- OPENAM-12173: NumberFormatException for AuthLevel in OAuth2 logs
- OPENAM-12174: XUI - Deleting a built-in authentication module will delete any other created by it
- OPENAM-12176: ServiceConfigManagerImpl does not retain order of notification events.
- OPENAM-12181: REST STS OIDC multi value local attributes not transformed into Claims correctly
- OPENAM-12184: Extend the DJ/DS SDK affinity LB feature to the userstore connection
- OPENAM-12186: Introspect endpoint for RPT does not check the authorization scheme
- OPENAM-12194: SLO with the SAML2 Auth Module PAP redirects to 'XUI/nullnull' when IDP has no SingleLogoutService defined
- OPENAM-12215: NPE thrown when calling OIDC authorize endpoint with invalid SSOToken
- OPENAM-12219: Resource leak in MonitoringAdapters#getMonAuthList
- OPENAM-12226: Device Match - server side script fails
- OPENAM-12232: Dynamic registration is not registering token_endpoint_auth_signing_alg, request_object_encryption_alg and request_object_encryption_enc
- OPENAM-12234: Values for objects of type com.sun.xml.bind.util.ListImpl are not printed in debug logs

- OPENAM-12244: Monitoring services unable to connect to Port
- OPENAM-12245: "Authentication by Module Instance" policy env condition doesn't work in session upgrade case
- OPENAM-12252: Delegated admin with Stateless Session, causes Admin Console failure.
- OPENAM-12254: ServiceListeners API doesn't always receive schema notifications
- OPENAM-12255: Process SMS notifications sequentially by default instead of using a threadpool
- OPENAM-12257: SMS listeners are not processed in the order they have been registered
- OPENAM-12258: ServiceSchemaManagerImpl can lose listeners when it gets invalidated
- OPENAM-12261: Honor org.apache.xml.security.ignoreLineBreaks=true when generating WS-Fed Assertions
- OPENAM-12262: CachedSMSEntry should only deregister its listener upon invalidation
- OPENAM-12293: Audit logging no longer logs REST operation details
- OPENAM-12315: NullPointerException after configuration store failover
- OPENAM-12319: Memory leak in accessing Jato Pages.
- OPENAM-12321: DeviceID showing extra info incorrectly in audit logs
- OPENAM-12328: Inefficient LDAP Search initiated by getRealmFromAlias() call as part of login process
- OPENAM-12333: AMIdentitySubject policy evaluation not cache when a lot of groups and datastore is use with delegated admin
- OPENAM-12338: policies?_action=evaluate checks all policy sets
- OPENAM-12357: ssoadmin tools distro include release canditate libraries
- OPENAM-12370: JWT verification fails when token idle time is too long
- OPENAM-12373: amster transport key makes rest operations too slow
- OPENAM-12377: WS-Fed extended metadata with unknown COT value should generate an error
- OPENAM-12380: client ip audit logging is not storing as IP but a list of IPs
- OPENAM-12384: Guice binding error when handling WSFed entities via ssoadm
- OPENAM-12401: DJLDAPv3Repo - insufficient debug logging to troubleshoot membership issues
- OPENAM-12403: LDAP response controls are not logged which complicates troubleshooting
- OPENAM-12412: Multi-valued LDAP attributes are not added to the OIDC id_token as expected

- OPENAM-12413: Enabled "'Return User DN to DataStore" of LDAP auth-module is resulting in one redundant search for "uid=uid=demo" in the configuration store
- OPENAM-12415: Self-Service KBA questions of TopLevel Realm(or Global Service) override SubRealm's
- OPENAM-12418: Unable to access Forgerock OATH for users with Profile when caching disable
- OPENAM-12419: Policy rules not updated when external configuration store connection restarted
- OPENAM-12440: User status is ignored
- OPENAM-12477: id_token requested using grant_type=authorization_code returns auth_time in milliseconds
- OPENAM-12498: Authorization Grant response returns scope(s) in the URL
- OPENAM-12511: User with the name "amadmin" can be created via the /users REST endpoint
- OPENAM-12514: IdP initiated SSO - NumberFormatException is raised in session upgrade case
- OPENAM-12531: Running webagent 5.0.0 against OpenAM 5.5.1 or later which is upgraded from previous version will result in segmentation fault or crash
- OPENAM-12533: Internal server error if JSON cannot be parsed by the json/authenticate endpoint
- OPENAM-12553: IdP Logout is ignored when using SAML2 Auth module and trying to use a goto
- OPENAM-12561: "Failed to create realm" with NullPointerException cause
- OPENAM-12610: AM cannot recognize version on upgrade from older versions
- OPENAM-12626: OIDC endSession endpoint does not call post authentication plugin onLogout functions
- OPENAM-12627: Initiating TransactionConditionAdvice with a wrong credential resulting in a non-error response
- OPENAM-12642: ServiceConfigManagerImpl does not implement equals/hashCode consistently
- OPENAM-12643: Notification listeners are stored in sets potentially allowing loss of listeners
- OPENAM-12644: ServiceConfigManagerImpl initialization is not synchronized correctly
- OPENAM-12645: Non-threadsafe fields are missing volatile keyword
- OPENAM-12646: SMSEmbeddedLdapObject initialization fails the first time with an NPE
- OPENAM-12647: SMS*LdapObject entriesPresent/NotPresent caches are access inconsistently
- OPENAM-12648: AgentsRepo instances are leaked during realm creation

- OPENAM-12649: Incorrect equality check in CachedSubEntries#notifySMSEvent
- OPENAM-12650: PluginSchemaImpl should clear CachedSMSEntry instance before throwing it away
- OPENAM-12651: Configuration objects not cleaned up as part of realm deletion
- OPENAM-12703: UnsupportedOperationException seen on SAML related session logout
- OPENAM-12770: Some SAML assertions are not deserialized from SAML2 Token.
- OPENAM-12784: ProviderConfiguration is not spec compliant
- OPENAM-12822: No URL resource is created for subsubrealms
- OPENAM-12826: WS-Federation extended metadata import fails when using ssoadm
- OPENAM-12866: Subsequent idpSSOInit calls after the first will fail if custom IDPAdapter forces auth step up
- OPENAM-12867: IdP-Proxy - Single Logout fails as LogoutResponse is not signed
- OPENAM-12898: DNS alias results in audience validation failure for clients authenticating using JWT
- OPENAM-12920: LDAPConnectionFactory is not closed when PersistentSearch is restarted
- OPENAM-12965: httpClient not exposed to OIDC Claim Script
- OPENAM-12972: SAML2 Auth Module fails with empty SAML2 Advice assertion.
- OPENAM-12984: Access Token Endpoint issues search request against datastore for OAuth Client
- OPENAM-12994: Unable to install AM using default configuration wizard when built with 'suppress-upgrade'
- OPENAM-12997: Consent for default scopes are not saved
- OPENAM-13000: Custom authentication module with a single ChoiceCallback value is processed without confirmation
- OPENAM-13006: Missing upgrade steps for OAuth2 ID Token Signing and Encryption Algorithms
- OPENAM-13008: Occasional shutdown error for AM
- OPENAM-13031: Failed search for non-existent user in datastore when fetching session properties and user profile is set to ignore
- OPENAM-13053: ScriptingService doesn't add the new values to whitelist during upgrade
- OPENAM-13064: OAuth2 - SAML v.2.0 Bearer Assertion Grant - SubjectConfirmationData element should be optional

- OPENAM-13072: Case Sensitive of Username Result in Listing UMA Resource Incorrectly
- OPENAM-13079: Import SAML2 MetaData for RoleDescriptor for AttributeQueryDescriptor fails
- OPENAM-13082: Address claim in default OIDC claims script outputs non-spec compliant format
- OPENAM-13085: WSFederation Active Request Profile authentication request hangs on input-less scripted modules
- OPENAM-13088: RFE: add option for isInitiator=false to WDSSO configuration
- OPENAM-13104: Introspection of access token fails when the wrong case of realm is used in the FIRST request
- OPENAM-13112: showServerConfig.jsp throw NullPointerException NPE when accessed using Site or LB URL
- OPENAM-13128: Invalid error message returned when user with expired password authenticates with persistent cookie module
- OPENAM-13151: OAuth2 Dynamic Registration does not accept Private-Use URI (for native apps) as redirect_uri
- OPENAM-13154: Lockout Duration Multiplier has no effect
- OPENAM-13162: Policy evaluation returns 403 with expired stateless app token
- OPENAM-13183: Concurrent changePassword requests to the "users" REST endpoint causes "insufficient access rights" failures
- OPENAM-13255: DefaultIDPAccountMapper does not append domain value for UPN
- OPENAM-13324: /users/{user}/devices/trusted REST queryFilter expression does not work and acts as "true"
- OPENAM-13330: Improve SessionReource Authz Module processing
- OPENAM-13359: P11RSAPrivateKey fails RSA key check.
- OPENAM-13398: SAML SSO broken after performing Session upgrade
- OPENAM-13407: AMIdentitySubject.isMember should not check privilege for group in different realm
- OPENAM-13411: Policy Configuration in Primary LDAP Server behaves different when there is one entry compared to many
- OPENAM-13426: EncryptSAMLIDPSPBasicAuthPwdStep fails in upgrade
- OPENAM-13430: Invalid request is returned instead of Invalid request parameter error
- OPENAM-13438: Setting org.forgerock.openam.ldap.heartbeat.timeout=-1 makes AM unusable

- OPENAM-13446: Social Auth Service doesn't redirect if already using another chain
- OPENAM-13465: Dynamic client registration sets wrong subjectType
- OPENAM-13490: Software Publisher Agent - Secret is not saved when creating an Agent
- OPENAM-13499: Incorrect transaction ID used in access events for CREST endpoints
- OPENAM-13511: DN Cache should be cleared after idRepo config change
- OPENAM-13530: Datastore Decision node removes username from shared state when it is not found
- OPENAM-13563: Help link on the "Services" XUI page points to out of date documentation
- OPENAM-13573: Concurrent changePassword requests to LDAPAuthUtils may cause "insufficient access rights" failures
- OPENAM-13574: Scripting class whitelist is missing classes after upgrade from 13.5.2 to 5.5.2
- OPENAM-13577: xmlsec 2.1.1.jar used in AM has issues when linebreaks enabled
- OPENAM-13578: KBA are not updatable after upgrade
- OPENAM-13582: token_endpoint_auth_signing_alg_values_supported not implemented
- OPENAM-13610: X-Frame-Options: SAMEORIGIN prevents use of check_session_iframe
- OPENAM-13612: OAuth2 CTS Grants without RefreshToken should expire with AccessToken timeout for one-to-one mapping
- OPENAM-13617: IDP initiated MNI requests to terminate link fail
- OPENAM-13670: Selfservice password reset token doesn't work in site due to OPENAM-6426
- OPENAM-13720: Public API method LDAPUtils.convertToLDAPURLs can not handle IPv6 literals
- OPENAM-13728: I can create new user with uid=testuser* after upgrade from 13.0.0
- OPENAM-13740: File descriptor / Connection leak when LDAP connection handshake fails/times out
- OPENAM-13741: After upgrade from 12.0.4 there are two additional service endpoints listed in API Explorer
- OPENAM-13750: HTTP 500 error when trying v3.1 /sessions in API explorer
- OPENAM-13779: Session API - _action=refresh requires an admin token
- OPENAM-13786: REST policy evaluation throws 500 Internal Error due to stateless ssotoken encryption alg conflict

- OPENAM-13793: Building AM with the suppress-upgrade causes an exception
- OPENAM-13838: Wording on "Maximum Caching Time" requires an update
- OPENAM-13842: OAuth2 Device flow - can no longer use user_code more than once
- OPENAM-13861: Social Authentication Tree does not complete its flow with ForceAuth parameter
- OPENAM-13890: Install.log logs AMLDAPUSERPASSWD for unprivileged demo user in plaintext
- OPENAM-13900: OAuth2 Device flow - duplicate user_code error after authenticating user
- OPENAM-13927: Some javadoc not generated
- OPENAM-13934: saml2error.jsp fails with exception when malformed SAML2 response given
- OPENAM-13978: Session Upgrade - AuthLevel format changes
- OPENAM-13991: 'issuer' value in .well-known/openid-configuration response is incorrect for a sub-realm
- OPENAM-13997: Include appropriate commons libraries in javadoc
- OPENAM-14022: We shouldn't be deploying Jetty inside a war file
- OPENAM-14040: LdifUtils debug logging prints out wrong classname
- OPENAM-14050: LDAP should reestablish connection to the orignal server after it has recovered
- OPENAM-14115: Sample Auth module does not work in a chain when used with Shared-state
- OPENAM-14138: Self registration url does not include realm parameter after upgrade from 13.5.1
- OPENAM-14147: arg=newsession in XUI just shows the "Loading..." page
- OPENAM-14167: HTML tags are shown part of the messages in Change Password section of AD Authentication module.
- OPENAM-14174: AM shows Ldapter.delete exception when session expires is triggered
- OPENAM-14175: CTS updates on multivalue attributes may throws Duplicate values exception
- OPENAM-14189: effectiveRange of Time environment has issue
- OPENAM-14232: Performance issue when creating resource_set in UMA with many existing resource_set
- OPENAM-14233: updated_at claim in the ID Token is returned as a string and not a number
- OPENAM-14239: FMSigProvider.verify NPE with null input for certificates
- OPENAM-14281: IdP Proxy relays wrong AuthnContextClassRef

- OPENAM-14307: ConcurrentModificationException when creating resource_set
- OPENAM-14308: LDAP Connection Pool Minimum Size for Identity Store missing from XUI
- OPENAM-14310: CheckSession page indicates the session is not valid
- OPENAM-14313: Audit Logging - STS transformations create duplicate entries
- OPENAM-14336: Unable to use Signed Metadata to Re-Import
- OPENAM-14337: Fail gracefully when request OIDC token using "Pairwise" Subject Type and no Redirection URI is configured in client
- OPENAM-14356: Deleting OAuth 2.0 Client triggers unfiltered search
- OPENAM-14369: Upgrading from OpenAM 13.5.0 with custom PAPs causes NPE failure
- OPENAM-14393: CTS Operation Fails Entry Already Exists logged for SAML2 Authentication is done
- OPENAM-14419: Policy evaluation returns search results for all policies that match outside of specified application
- OPENAM-14427: Certificate Module with option "Match Certificate in LDAP" does not work
- OPENAM-14450: userinfo typo in Claims.java
- OPENAM-14465: SAML2 Artifact binding fails on multi-instance / multiserver IDP setup with SAML2 Failover on
- OPENAM-14466: Logs show MissingResource for key unableToCreateArtifactResponse during SAML2 login
- OPENAM-14523: NullPointerException in IdP-initiated ManageNameIDRequest using SOAP Binding
- OPENAM-14539: SAML SLO with multi protocols
- OPENAM-14546: SSOADM access not audited to the ssoadm.access logs anymore
- OPENAM-14572: prompt=login destroys and creates new session
- OPENAM-14581: Handling ManageNameID fails if NameID does not include SPNameQualifier
- OPENAM-14642: OIDC Dynamic Client Registration registration_client_uri uses only Host header not BaseURL
- OPENAM-14643: OIDC Dynamic Client Registration registration_client_uri does not work for root realm
- OPENAM-14694: Consent page still shows claim values even when supported claim description is omitted

- OPENAM-14707: ConsentRequiredResource class does not reuse value in Base url source service
- OPENAM-14740: idpSingleLogoutRedirect throws error 500 IllegalStateException on SLO
- OPENAM-14744: Multivalued DN stops persistent search
- OPENAM-14766: introspect and tokeninfo endpoints return Internal Server Error 500 in some invalid tokens
- OPENAM-14786: idpSingleLogoutPOST throws error 500 IllegalStateException on SLO
- OPENAM-14799: Unable to update Agent profile using REST
- OPENAM-14825: OAuth2 Dynamic Registration with Software Statement triggers objectClass=* search
- OPENAM-14829: AuthSchemeCondition doesn't return realm aware policy condition advice
- OPENAM-14842: Misleading "CTS: Operation failed: Result Code: Connect Error" message when CTS store is still up and running
- OPENAM-14858: When NameIDPolicy does not contain `Format=..`, remoteEntityID is passed as null
- OPENAM-14867: AuthType is not set for Authentication Tree (AnyKnownUserAuthzModule fails in AuthTree)
- OPENAM-14874: It would be nice if the x-forwarded-* option was able to parse the comma-separated string and use the first (outermost) proxy host name.
- OPENAM-14883: OAuth2/OIDC - Issuing client secret to Public clients during registration
- OPENAM-14929: idpSSOInit error when session authLevel does not map to Auth Context
- OPENAM-14939: Enable "org.apache.xml.security.ignoreLineBreaks=true" by default
- OPENAM-14940: Improve SAML2 Response/Assertion generation to not have carriage return inbetween XML tag
- OPENAM-14973: Monitoring throws StackTrace even if JDMK isn't being used/needed.
- OPENAM-14977: PKCE Code challenge method for Authorization Code if not set should use plain
- OPENAM-14986: AM Cannot connect to TLSv1.2 DJ server (production mode) after JDK 8 update 192
- OPENAM-14989: Configuring Rest STS with a delegated admin fails
- OPENAM-15012: OIDC - JWT Request Parameter returns errors in query, not in the fragment
- OPENAM-15044: OpenID connect id_token bearer Module Unable to obtain SSO Token due to OpenIDResolver Caching

- OPENAM-15073: Missing RelayState query parameter in the AM redirect to fedlet application
- OPENAM-15089: SAML SLO - Allow RelayState to be a path-relative URL
- OPENAM-15116: Auth ID jwt can be modified to determine whether a realm exists or not
- OPENAM-15147: HTTP 500 upon accessing openam/json/
- OPENAM-15164: CDSSO with "ignore profile" throws "No OpenID Connect provider"
- OPENAM-15198: WS-FED Attribute Mapper returns incorrect map when AM is SP
- OPENAM-15210: Authentication nodes that is assigned AuthType values may not work in Session Upgrade case with custom modules
- OPENAM-15216: LDAP Decision Node does not continue through "Fail" flow when Node Fails with exception
- OPENAM-15244: AM configuration does not perform schema extension for identity store although it has the permissions
- OPENAM-15257: XUI freezing when /authenticate returns unhandled http result codes
- OPENAM-15286: Upgrade from 12.0.4 fails
- OPENAM-15307: Trees Example is not working as expected OOTB to ?service=Example
- OPENAM-15363: Redirect_uri_mismatch error occurs in Agent 5.x after upgrading from OpenAM 13.5.0
- OPENAM-15432: Oath User Devices endpoint not accessible for delegated admin
- OPENAM-15444: Prepare for Chrome's move to SameSite=lax by default
- OPENAM-15446: Incorrect error management during SAML SSO
- OPENAM-15459: When Encrypted Attributes on SP is set only with AutoFederation enabled, the attributes get decryption error
- OPENAM-15483: IDPSSOUtil.doSSOFederate throws NumberFormatException when subrealm is used with federation
- OPENAM-15487: OIDC - JWT Request Parameter returns errors in query, not in the fragment with invalid acr essential claim
- OPENAM-15494: AM expects nonce request parameter in authorize request when no id_token will be returned
- OPENAM-15507: 500 error when calling /revoke or /refresh endpoint with wrong token
- OPENAM-15510: Generic amster error message "No Base Entity dc=config,dc=forgerock,dc=com found" needs to detail the actual ldap error - during install-openam

- OPENAM-15533: WS-Federation doesn't work with Authentication Trees
- OPENAM-15559: OATH module broken in Japanese locale
- OPENAM-15562: SAML2 crosstalk fails when Accept-Language header is missing from the original request
- OPENAM-15651: AM 5.5.2 copyrights displayed in XUI pages out of date
- OPENAM-15652: Debug.jsp does not update all existing appenders when trying to override -Dcom.iplanet.services.debug.level at runtime
- OPENAM-15694: RestSTSServiceHttpRouteProvider causes memory leak by adding route for every access
- OPENAM-15713: AM SP drop the 80 characters RelayState silently for HTTP Redirect
- OPENAM-15722: SAML2 IdP federation endpoint does not set amlbcookie when using host-based cookies
- OPENAM-15724: SAML2 entities do not set amlbcookie if there is only one server
- OPENAM-15776: Push Registration fails (QR code invalid) to register
- OPENAM-15805: idtokeninfo endpoint gives invalid signature error when ID Token is expired
- OPENAM-15841: DisableSameSiteCookiesFilter broken on WebLogic
- OPENAM-15849: An admin cannot DELETE 2fa devices owned by users
- OPENAM-15853: External UMA store fails on resource creation
- OPENAM-15896: WS-Federation relying party initiated passive request - stuck at Account Realm selection
- OPENAM-15899: Have an option to add <ds:X509Certificate> tag in the signed SLO request
- OPENAM-15900: Kerberos fails when used with IBM JDK
- OPENAM-15944: WS-Federation - RPSignin Request fails because config data is used unchecked
- OPENAM-15982: OIDC - JWT Request Parameter returns errors in query, not in the fragment when consent is denied

Key Fixes in AM 5.5.1

- OPENAM-11988: HTTP 500 when validating SSO tokens if API version is omitted in AM 5.5

Key Fixes in AM 5.5.0

- OPENAM-11834: Passwords being set to empty strings in tabbed forms in XUI

- OPENAM-11646: Cookie values wrapped in double quotes
- OPENAM-11632: CDCServlet does not work with realm
- OPENAM-11610: WindowSSO module broken in AM 5.1.1 after upgrade
- OPENAM-11526: Realm Authentication chain post authentication classes PAP not triggered on chains with multiple modules
- OPENAM-11391: Requesting 'OAuth2.0/OIDC' auth module a second time results in display of AM's "Authentication Failed" page
- OPENAM-11300: OIDC request parameter is failing when message level is enabled
- OPENAM-11280: authentication with noSession=true fails if post authentication plugin class is present
- OPENAM-11218: OpenAM throws service error for Application Module
- OPENAM-11217: SAML2 Authentication module is not invoking custom SP Adapter class implementing a preSingleSignOnRequest() method
- OPENAM-11196: Incorrect debug logging level used in FMEncProvider.getEncryptionKey
- OPENAM-11154: Memory leak in SMSEventListenerManager#subNodeChanges
- OPENAM-11115: Push authentication should use alias attributes to find identities
- OPENAM-11101: Social Auth links do not contain the goto url
- OPENAM-11070: Need OAuth2 authentication to work in Android with implied consent
- OPENAM-11057: Global User Self Service UI does not display values
- OPENAM-11015: ForceAuth session upgrade does not work
- OPENAM-10971: FR-OATH auth module can not be used in auth chain if the username in sharedstate map does not 'match' the search attribute of the data store
- OPENAM-10970: logout response binding should be selected based on the capabilities of the SP
- OPENAM-10965: Stateless OAuth2 can't verify access and refresh token
- OPENAM-10931: IdentitySubject not adding isMember() result to cache after entry has changed.
- OPENAM-10782: endSession with an id_token generated from a refresh_token request does not destroy the session
- OPENAM-10756: setSucessModuleNames in AMLoginModule calls AuthModule's getPrincipal multiple times
- OPENAM-10585: The "claims" Request Parameter from the openid standard isn't functional

- OPENAM-10578: Stateless access token doesn't contain the grant type
- OPENAM-10562: Audit log 'Configuration' entries are not written when using external configuration store
- OPENAM-10332: Quota constraints exceeded - Interim Fix
- OPENAM-10129: OAuth2 Device flow - user code verification is case insensitive
- OPENAM-10103: output from re-indexing action during initial configuration is lost
- OPENAM-10102: insufficient progress information during configuration
- OPENAM-10013: HOTP session upgrade not possible in XUI if the wrong code is entered first time
- OPENAM-9979: Authentication chain post authentication classes are not used if realm level PAP setting exists
- OPENAM-9885: Oauth2 load: Tomcat keeps logging "WARNING: Addition of the standard header "Pragma" is discouraged as a future version of the Restlet API will directly support it"
- OPENAM-9156: 'Not Found' error in UI when opening a custom auth module created with ssoadm with the name the same as type
- OPENAM-8771: "Unknown Error: Please contact your administrator", shown with FacebookSocialAuthentication option "Prompt for password setting and activation code" (org-forgerock-auth-oauth-prompt-password-flag)
- OPENAM-8270: Using client_credentials Grant type with openid scope returns User must be authenticated to issue ID tokens
- OPENAM-8063: Merge Debug Files feature does not work correctly
- OPENAM-7781: persistent cookie auth module does not allow to change cookie name by default
- OPENAM-7437: Finish button of Identity Provider wizard doesn't work
- OPENAM-5864: Quota constraints exceeded in multi-instance with LB and CTS enabled
- OPENAM-5153: Auth modules should call setAuthLevel after successful login
- OPENAM-5152: AMAuthLevelManager miscalculates auth level
- OPENAM-3679: IDP Finder fails to validate relaystate
- OPENAM-1325: OpenAM fails to setup when deployed under the root uri ('/')

5.2. Limitations

The following limitations and workarounds apply to AM 5.5:

Limitations in AM 5.5.2

- There are no limitations in functionality other than those listed in Limitations in AM 5.5.0.

Limitations in AM 5.5.1

- There are no limitations in functionality other than those listed in Limitations in AM 5.5.0.

Limitations in AM 5.5.0

- **Server Error When OAuth 2.0 or OpenID Connect Clients Request Access Tokens**

  OAuth 2.0 or OpenID Connect client using HMAC for signing JSON web tokens may encounter the following issues:

  - REST calls requesting access tokens return `server_error`
  - There are errors in AM's logs resembling the following:

    ```
    ERROR: Failed to update JwkStore for jwks URI https://openam.example.com:8443/am/oauth2/customers/
    connect/jwk_uri
    org.forgerock.json.jose.exceptions.FailedToLoadJWKException: Unable to load the JWK location over HTTP
    at org.forgerock.json.jose.jwk.JWKSetParser.gatherHttpContents(JWKSetParser.java:84)
    at org.forgerock.json.jose.jwk.JWKSetParser.jwkSet(JWKSetParser.java:96)
    at org.forgerock.json.jose.jwk.store.JwksStore.reloadJwks(JwksStore.java:85)
    ```

  To work around this issue, navigate to Realms > *Realm Name* > Applications > OAuth 2.0 > Clients > *Client Name* > Signing and Encryption and perform one of the following steps:

  - Leave the Json Web Key URI field blank, removing the default value. HMAC signing does not require a JWK URI.
  - Ensure the URL specified in the Json Web Key URI field is resolvable.

- **Using the Documented CORS Filter With IDM Integration Causes Errors**

  When configuring IDM to delegate authentication to AM, as described in the IDM *Samples Guide*, you must configure AM with a cross-origin resource sharing (CORS) filter.

  However, when you use a CORS filter based on the `org.forgerock.openam.cors.CORSFilter` filter class, Unexpected End of JSON Input errors occur.

  To work around the problem, configure AM's `web.xml` file as described in "Enabling CORS Support" in the *Installation Guide*, but use a CORS filter specific to the AM web container instead of using a filter based on the `org.forgerock.openam.cors.CORSFilter` filter class. For example, for Apache Tomcat, use a filter based on the `org.apache.catalina.filters.CorsFilter` filter class:

  - Add a `filter` clause similar to the following to the `web.xml` file, making sure to specify the correct URLs for your deployment in the `cors.allowed.origins` parameter:

```
<filter>
    <filter-name>CORSFilter</filter-name>
    <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
    <init-param>
        <param-name>cors.allowed.headers</param-name>
        <param-value>Content-Type,X-OpenIDM-OAuth-Login,X-OpenIDM-DataStoreToken,X-Requested-
With,Cache-Control,Accept-Language,accept,Origin,Access-Control-Request-Method,Access-Control-Request-
Headers,X-OpenAM-Username,X-OpenAM-Password,iPlanetDirectoryPro</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.methods</param-name>
        <param-value>GET,POST,HEAD,OPTIONS,PUT,DELETE</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.origins</param-name>
        <param-value>https://openam.example.com:8443,https://openidm.example.com:8443</param-value>
    </init-param>
    <init-param>
        <param-name>cors.exposed.headers</param-name>
        <param-value>Access-Control-Allow-Origin,Access-Control-Allow-Credentials,Set-Cookie</param-
value>
    </init-param>
    <init-param>
        <param-name>cors.preflight.maxage</param-name>
        <param-value>10</param-value>
    </init-param>
    <init-param>
        <param-name>cors.support.credentials</param-name>
        <param-value>true</param-value>
    </init-param>
</filter>
```

- Add the following `filter-mapping` clause to the `web.xml` file:

```
<filter-mapping>
    <filter-name>CORSFilter</filter-name>
    <url-pattern>/json/*</url-pattern>
</filter-mapping>
```

- **JCEKS Keystore Support for User Self-Services**

  In OpenAM 13.0.0, the user self-service feature is stateless, which means that the end-user is tracked and replayed by an encrypted and signed JWT token on each AM instance. It also generates key pairs and caches its keys locally on the server instance.

  In a multi-instance deployment behind a load balancer, one server instance with the user self-services enabled will not be able to decrypt the JWT token from the other instance due to the encryption keys being stored locally to its server.

  OpenAM 13.5.0 and later solve this issue by providing a JCEKS keystore that supports asymmetric keys for encryption and symmetric keys for signing. Users who have installed OpenAM 13.0.0 and enabled the user self-service feature will need to run additional steps to configure a JCEKS keystore to get the user self-service feature operating after an upgrade.

For specific instructions to configure the JCEKS keystore, see "Configuring Keystores" in the *Setup and Maintenance Guide*.

Note

This procedure is not necessary for the following users:

- Users upgrading from versions prior to OpenAM 13.0.0 are not impacted.
- Users who upgrade from OpenAM 13.0.0 and do not enable the user self-services feature are not impacted.
- Users who do a clean install of OpenAM 13.5.0 or later are not impacted.

- **Cached JavaScript Files from OpenAM 12.0.0 May Cause Redirect to undefined:8080**

  If you configure an OpenAM 12.0.0 instance with long-lived cache times for the `/XUI/index.html` file, you may experience unexpected redirects to `undefined:8080` after upgrading.

  To work around this issue, in your chosen web container, or proxy server, reconfigure the cache time for the `/XUI/index.html` file to be short-lived, for example, 5 minutes. Allow enough time that cached files with the long-lived cache time will have expired before upgrading.

  Note

  This issue does not affect upgrades from OpenAM 12.0.1 or later. OpenAM 12.0.1 and later set a short-lived `cache-control` header on UI files to work around the problem of having stale files cached locally.

- **RADIUS Service Only Supports Commons Audit Logging**. The new RADIUS service only supports the new Commons Audit Logging, available in this release. The RADIUS service cannot use the older Logging Service, available in releases prior to OpenAM 13.0.0.

- **Administration Console Access Requires the `RealmAdmin` privilege**

  In this version of AM, administrators can use the AM console as follows:

  - Delegated administrators with the `RealmAdmin` privilege can access full AM console functionality within the realms they can administer. In addition, delegated administrators in the Top Level Realm who have this privilege can access AM's global configuration.
  - Administrators with lesser privileges, such as the `PolicyAdmin` privilege, can not access the AM administration console.
  - The top-level administrator, such as `amadmin`, has access to full AM console functionality in all realms and can access AM's global configuration.

5.3. Known Issues

The following important known issues remained open at the time release 5.5 became available. For details and information on other issues, see the issue tracker.

Known Issues in AM 5.5.2

- OPENAM-12249: Unable to create sub-realms if the parent contains an Inner Tree
- OPENAM-12251: API Descriptor using String instead of "Number" type for some settings
- OPENAM-12357: ssoadmin tools distro include release canditate libraries
- OPENAM-12436: The ../sessions?_action=validate endpoint always resets the session's idle time
- OPENAM-12495: When delete an identity it is not being removed from the groups
- OPENAM-12506: Upgrade could fail with RemoveReferralsStep having too broad base DN
- OPENAM-12625: JWT OIDC Token can't be valid for over 86400 seconds
- OPENAM-12666: Agent OAuth 2 provider does not support custom login URLs
- OPENAM-12690: XUI Theme Configuration Realm Mapping is Case Sensitive
- OPENAM-12713: Subrealm creation fails if an Inner Tree is present
- OPENAM-12729: Prometheus and CREST monitoring endpoint config upgrade step required
- OPENAM-12759: max_age should a number, not a string
- OPENAM-12801: OAuth2 token signing forces PKCS#11 keys to have specific attributes
- OPENAM-12847: Public API broken - SSOTokenManager.getValidSessions(SSOToken requester, String server)
- OPENAM-12946: CTSBlacklist performs initial (and most expensive) search twice
- OPENAM-12955: Resource Owner Password Credentials Grant does not work with trees
- OPENAM-12985: debug log files are swamped with message 'LDAPUtils.isDN: Invalid DN' in 'error' level
- OPENAM-12996: Config upgraded from AM 5.5.1 containing trees fails to be imported
- OPENAM-13291: Create Identities Page appears broken after upgrade from 5.5 (to 6.0 or 6.5)
- OPENAM-13434: grant_types_supported is not returned in the well-know and this is not optional
- OPENAM-13435: token_endpoint_auth_signing_alg_values_supported not populated in the well-known

- OPENAM-13436: userinfo_signing_alg_values_supported not populated in the well-known
- OPENAM-13481: Stateless OAuth2 Client_credential grant/implicit type has long CTS token timeout
- OPENAM-13732: Session Remaining Time is displayed with more precision and not rounded up
- OPENAM-13831: RP-Initiated Logout does not handle state parameter
- OPENAM-13892: Erroneous "Response's InResponseTo attribute is not valid error "SAML2 failover is enabled" when it is not
- OPENAM-14018: Radius Authentication Module Primary and Secondary Radius Server help button shows server:port when it should be server
- OPENAM-14112: Using client-based sessions when acting as SP can lead to an out-of-date client-based session cookie
- OPENAM-14167: HTML tags are shown part of the messages in Change Password section of AD Authentication module.
- OPENAM-14231: Passing in a JWT (with jku in the header) to the authorize endpoint fails
- OPENAM-14503: SAML2 - Key Transport Algorithm - RSA OAEP must be supported
- OPENAM-14534: The request parameter should accept any signing algorithms supported by the OP
- OPENAM-14545: Debug log showing NullPointerException in com.sun.identity.federation.common.FSUtils#getRemoteServiceURLs
- OPENAM-14848: Insufficient debug logging in OpenID Connect authentication module
- OPENAM-14865: No error message is provided when login page is supplied with incorrect session cookie domain
- OPENAM-14919: Unncessary 'Unable to parse packet received from RADIUS client' log entries in log file
- OPENAM-14938: ID repo setAttributes service call returns the wrong error message with multiple datastores
- OPENAM-14995: IdP Initiated single logout only performs local logout if IdP session cannot be found in cache
- OPENAM-15036: Cannot view/manage SAML IdP entity in console, imported from schema compliant meta data file
- OPENAM-15117: KeyVault KeyStoreType not supported
- OPENAM-15129: registering client with token_endpoint_auth_method=none returns secret
- OPENAM-15145: OpenAM Scope Validator calls getUserInfo twice when creating IdToken

- OPENAM-15275: user with the name "amadmin" can be created via legacy UI
- OPENAM-15425: OIDC endsession - encrypted id_tokens are not supported
- OPENAM-15667: AM debug log does not tell which auth-module was handled - needed for troubleshooting
- OPENAM-15670: DeviceIdSave auth module initialization fails if username is null
- OPENAM-15744: com.sun.identity.enableUniqueSSOTokenCookie=true results in infinite redirects
- OPENAM-15809: Update CORS service for IE11 compatibility

Known Issues in AM 5.5.1

- There are no known issues other than those listed in Known Issues in AM 5.5.0.

Known Issues in AM 5.5.0

- OPENAM-4713: Can't use Common Tasks wizards when logged in as a delegated administrator
- OPENAM-9012: LDAP connection heartbeat settings should be also added to policy configuration
- OPENAM-9931: Global Session Service - two fields with the exact same name
- OPENAM-11194: Goto url not used in the presence of a valid session or after a redirect callback
- OPENAM-11737: http.response.headers not populating in audit logs
- OPENAM-11741: NPE in admin console when accessing parts with old UI
- OPENAM-11746: Syslog data is not fully RFC compliant
- OPENAM-11921: Incorrect NameId Format offered for SAML2 auth module in console
- OPENAM-11925: CORSFIlter causings failures after moving to 5.x from 13.5.x
- OPENAM-11937: Federation UI does not allow empty NameIDMappingService
- OPENAM-11956: SAML2 RelayState values are seen as invalid if they are not a URL which appears to go against the spec
- OPENAM-11980: Social OIDC wizards do not work when provisioning accounts locally

Chapter 6
Documentation Updates

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

Documentation Change Log

Date	Description
	Initial release of AM 5.5.2. The following documentation changes were made: • Added a note that we do not recommend more than one writeable repo per realm. For more information, see "Important Considerations for Using External Identity Repositories" in the *Installation Guide*. • Added documentation for PKCE (RFC 7636) support. For more information, see OAuth 2.0 in the *OAuth 2.0 Guide*. • Added clarification that `amAdmin` is a special built-in account, and that to use functionality that uses a user profile, such as Device Match or Push notifications, you should create users or groups, and delegate administrator privileges to them. For more information, see "Web-Based AM Console" in the *Setup and Maintenance Guide*. • Added an example using `authIndexType`. For more information, see "Authentication and Logout" in the *Development Guide*. • Updated the Installation Guide with an extra ACI requirement when running DS in production mode. For more information, see "Non-Admin User Creation and ACI Import" in the *Installation Guide*. • Add the option, `--offline`, to the **rebuild-index** command examples. For more information, see "*Supported Scripts*" in the *Installation Guide*. • Add documemtation that JWT Bearer claims for client authentication have a TTL of 30 minutes (non-configurable). For more information, see "JWT Bearer Profile" in the *OAuth 2.0 Guide*. • Removed the section on the third-party sample RADIUS client, which we no longer ship. • Removed `iPlanetDirectoryPro` header in the REST-STS translate examples. For more information, see "Security Token Service Process Flows" in the *Security Token Service Guide*.

Date	Description
	• Added additional JSON responses for all settings of "Destination After Successful Self-Registration". For more information, see "To Register a User with the REST APIs" in the *User Self Service Guide*. • Removed references to the deprecated endpoint, `/ffrest`. For more information, see "OAuth 2.0 Token Administration Endpoint (Legacy)" in the *OAuth 2.0 Guide*. • Added a note that sticky load-balancing is required in a load balancer deployment. For more information, see "Things to Consider When Installing Multiple Servers" in the *Installation Guide*. • Add documentation on how to generate a list of ACIs. For more information, see "To Prevent Anonymous Access in External Configuration Stores" in the *Installation Guide*. • Updated the documentation so that `configstorepwd` and `dsameuserpwd` now use `.keypass` instead of `.storepass`. For more information, see "To Change Key Aliases' Passwords" in the *Setup and Maintenance Guide*. • Removed references to Oracle WebLogic required packages, Bouncy Castle and Jackson packages, which is not included by default. For more information, see "To Prepare for Oracle WebLogic" in the *Installation Guide*. • Updated the WebLogic chapter for installation. For more information, see "To Prepare for Oracle WebLogic" in the *Installation Guide*. • Added expire header information in the preparing Tomcat section. For more information, see "Preparing Apache Tomcat" in the *Installation Guide*. • Add an entry for the `One Time Password Max Retry` parameter. For more information, see "ForgeRock Authenticator (OATH) Authentication Module Properties" in the *Authentication and Single Sign-On Guide*. • Update documentation for configuring CTS connection pool size. For more information, see "Tuning CTS LDAP Connection Settings" in the *Setup and Maintenance Guide*. • Fixed the ACI example in CTS preparation. For more information, see "To Create a Non-Admin User" in the *Installation Guide*. • Removed mention of the Federation Connectivity Test, which no longer exists. • Added a note about opening the JCEKS keystore during upgrade. For more information, see "Keystore Configuration After Upgrade" in the *Setup and Maintenance Guide*. • Corrected text for startup settings. For more information, see "To Override Startup Settings by Using Java Properties" in the *Installation Guide*. • Updated documentation that the Liberty Identity Framework is marked as deprecated since AM 5.0.

Date	Description
	• Added a tip about account lockout being triggered by counting invalid password exceptions. For more information, see "The Sample Authentication Logic" in the *Authentication and Single Sign-On Guide*. • Updated documentation that LDAP group and user container property can be empty. For more information, see "Data Store Configuration Properties" in the *Setup and Maintenance Guide*. • Added the `isInitiator` parameter for the JDK Kerberos LoginModule. For more information, see "Authentication Module Properties" in the *Authentication and Single Sign-On Guide*. • Updated the documentation to add an optional ACI step if DS is in production mode. For more information, see "To Create a Non-Admin User" in the *Installation Guide*. • Simplified the session logout section and corrected curl examples. For more information, see "Invalidating Sessions" in the *Authentication and Single Sign-On Guide*. • Added a warning that if AM cannot access the CTS token store, users will be unable to log in to the AM module. For more information, see "CTS Configuration" in the *Installation Guide*. • Added an entry for a new property, `Affinity Enabled`. For more information, see "External Store Configuration" in the *Reference*. • Fixed the example for logging out a session using a session handle. For more information, see "logoutByHandle" in the *Development Guide*. • Updated documentation to alter scopes used in UMA examples to avoid clashing with an earlier policy. For more information, see "Register Resource Sets" in the *User-Managed Access (UMA) 2.0 Guide*. • Updated the text that `sunserviceID` needs to be indexed when there are a large number of OAuth2 clients or if any agents are registered on their system. For more information, see ForgeRock Knowledge Base. • Added information on a new property, `org.forgerock.allow.http.client.debug`. For more information about this property, see "Advanced Properties" in the *Reference*.
2018-05-17	Added a procedure to configure **ssoadm** when using AES key wrap encryption. For more information, see "To Configure ssoadm for AES Key Wrap Encryption" in the *Installation Guide*. Added an admonition about enabling the `org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH`. For more information, see "Preparing Apache Tomcat" in the *Installation Guide*.
2018-05-04	Updated the following information about stateless sessions across the guides:

Date	Description
	• It was stated that the same AM server could process fewer stateless sessions than stateful sessions in the same time. This information was incorrect based on ForgeRock's internal testing. • It was stated that the size of the stateless cookie was ten times larger than the size of the stateful cookie. This information was incorrect. The size of the stateless cookie varies depending on the signing, encryption, and compression algorithms applied to it. • It was stated that stateless sessions do not require sticky load balancing. While this information is correct, the documentation has been amended to specify that AM caches the decrypt sequence of the cookie to improve performance and, therefore, stateless sessions benefit from sticky load balancing.
2018-02-06	Added a note that the JWT expiry lifetime is set to 30 minutes maximum. For information, see "JWT Bearer Profile" in the *OAuth 2.0 Guide*.
2018-01-18	Added documentation on about a new OATH/HOTP property, `One Time Password Max Retry` that allows you to configure the number of retry attempts for the OTP. For information, see "OATH Authentication Module Properties" in the *Authentication and Single Sign-On Guide* and "HOTP Authentication Module Properties" in the *Authentication and Single Sign-On Guide*.
2017-10-31	Added information about the need to update the script or Maven `pom.xml` file used to build a custom authentication module when the module uses a service loader. See "Important Changes to Existing Functionality".
2017-10-27	Initial release of Access Management 5.5.1

Appendix A. Release Levels and Interface Stability

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

A.1. 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

A.2. ForgeRock Product Interface Stability

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

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

Interface Stability Definitions

Stability Label	Definition
Stable	This documented 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 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.
Deprecated	This interface is deprecated and likely to be removed in a future release. For previously stable interfaces, the change was likely announced in a previous release. Deprecated interfaces will be removed from ForgeRock products.
Removed	This 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 evolving new technology that are not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to

Stability Label	Definition
	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 interfaces can change without notice. If you depend on one of these interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.

Appendix B. Getting Support

For more information or resources about AM and ForgeRock Support, see the following sections:

B.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.

B.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.

B.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.