Release Notes

/ ForgeRock Access Management 6

Latest update: 6.0.0.7

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. Patch Bundle Releases

AM 6.0.0.7

- ForgeRock patch bundle releases contain a collection of fixes that have been grouped together and released as part of our commitment to support our customers. AM 6.0.0.7 is the latest patch bundle release targeted for AM 6.0.0.x deployments and can be downloaded from the *ForgeRock Backstage* website. To view the list of fixes in this release, see Key Fixes in AM 6.0.0.7.

  The AM 6.0.0.7 patch bundle release is cumulative and contains all the fixes included in previous 6.0.0.x releases (see "*Fixes, Limitations, and Known Issues*"). The release can be deployed as an initial deployment or updated from an existing 6.0.0.x deployment, see "Supported Upgrade Paths". AM 6.0 is available for download at the *ForgeRock Backstage* website.

  For general information on ForgeRock's maintenance and patch releases, see Maintenance and Patch Availability Policy.

1.2. New Features

ForgeRock Access Management 6 is a major release that introduces new features, functional enhancements, and fixes.

New Features in AM 6

- **Intelligent Authentication**

  Intelligent Authentication is based on a powerful decision tree framework, consisting of *authentication trees* made up of *authentication nodes*.

  Combining authentication nodes into authentication trees enables you to:

  - Configure, measure, and adjust login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors.

- Consume out-of-the-box authenticators, utilize existing authenticators, and integrate with cyber security solutions with an intuitive drag-and-drop interface — all in one place.
- Leverage user login analytics to increase user adoption rates, and improve the customer experience.
- Redirect suspicious users for further monitoring.
- **New Authentication Nodes**

  AM 6 adds a number of authentication nodes for various use cases, including:

  - Social Authentication. Authenticate to AM with Facebook, Google, or any OAuth 2.0-compliant social identity provider.
  - Account Provisioning. Create local accounts, assume an Anonymous role, or hand off provisioning to ForgeRock Identity Management.
  - Multi-factor Authentication. Increase confidence when authenticating by using multiple factors, such as one-time passwords or push notifications.
  - Authentication Monitoring. Add monitoring nodes to the tree to track metrics for the various authentication flows you offer.
  - Logout Monitoring. Add a webhook to an authentication session that posts information to an endpoint when a user logsout or their session becomes invalidated.

  For more details of the nodes available in AM 6, see "Configuring Authentication Nodes" in the *Authentication and Single Sign-On Guide*.

  Tip

  In addition to the nodes that are included in AM 6, a number of authentication nodes are available from the ForgeRock Marketplace website.

- **Distributed Login**

  AM 5.x stores authentication trees and chains authentication sessions in its memory. This requires a load balancer set up for session stickiness in front of the AM site to ensure that the authentication flow is always directed to the same AM server.

  AM 6 removes the constraint of storing authentication sessions in memory when using authentication trees, which allows any AM server to satisfy any part of an authentication tree flow. Therefore, this change removes the requirement of sticky load-balancing when using authentication trees.

To handle the authentication tree flow in a distributed way, AM 6 can store authentication sessions in the same way it stores authenticated user's sessions:

- In the CTS token store, accessible by any AM server in the site.
- In the client, as an encrypted JWT.

Authentication trees can still handle the authentication flow in a centralized way by storing authentication sessions in AM's memory, which is the default configuration for a realm after an AM upgrade.

To protect authentication sessions from malicious users that may want to replay parts of the authentication flow and retry specific authentication nodes, AM 6 introduces authentication session whitelisting.

For more information, see:

- "About Sessions" in the *Authentication and Single Sign-On Guide*
- "*Implementing Sessions*" in the *Authentication and Single Sign-On Guide*

- **OAuth 2.0**
  - **Dynamic OAuth 2.0 Scopes**

    AM 6 allows granting or denying OAuth 2.0 scopes based on authorization policies. When requesting an access token, AM's Authorization Service grants or denies scopes dynamically by evaluating authorization policies defined in the Default OAuth2 Scopes Policy Set, `oauth2Scopes`.

    The principal advantage of granting or denying scopes dynamically is that a single OAuth 2.0 client configured for a comprehensive list of scopes can serve different scope subsets to resource owners based on policy conditions.

    By default, OAuth 2.0 grants are not configured to interact with the Authorization Service. The high-level steps to enable this new feature are as follows:

    - Enable Use Policy Engine for Scope decisions in the OAuth2 Provider Service.
    - Create policies in the Default OAuth2 Scopes Policy Set, `oauth2Scopes`.

      Creating OAuth 2.0 policies follows the same principles as creating any other authorization policy.

    For more information, see:

    - "Resource Types, Policy Sets, and Policies" in the *Authorization Guide*
    - "Policy Decisions" in the *Authorization Guide*

- "Configuring Policies" in the *Authorization Guide*
- "Implementing OAuth 2.0 Policies" in the *Authorization Guide*

- **General**
  - **Endpoint Cross-Site Request Forgery (CSRF) Filter**

    Access Management 6 includes a new CSRF filter that applies to all REST endpoints under the `json/` root. It requires that all requests other than GET, HEAD, and OPTIONS have, at least, one of the following headers:

    - `X-Requested-With`
    - `Accept-API-Version`

    Important

    The filter is enabled by default. REST requests other than GET, HEAD, and OPTIONS made to endpoints under the `json/` root will return `403 Forbidden` messages unless one of the headers is included.

    For more information, see "Cross-Site Request Forgery (CSRF) Protection" in the *Setup and Maintenance Guide*.

  - **Forgotten Password Account Lockout Feature**

    AM 6 provides new properties to limit the number of attempts allowed at answering security questions (KBA), and to lock the account if exceeded. The properties are as follows:

    - Enforce password reset lockout (`forgotten.password.kba.number.of.allowed.attempts.enforced`)
    - Lock Out After number of attempts (`forgotten.password.kba.number.of.allowed.attempts`)

    Important

    To support these new properties, the user data store must contain the appropriate schema. New AM 6 installations already account for the change in the schema, but you must perform but you must upgrade the user data store schema in earlier versions of OpenAM or AM.

    For more information about the required upgrade steps, see "*Upgrading Servers*" in the *Upgrade Guide*.

    For more information about configuring the forgotten password user self-service feature, see "Configuring the Forgotten Password Reset Feature" in the *User Self-Service Guide*.

  - **New Password Replay Post-Authentication Plugin Class**

    AM 6 introduces a more secure password replay post-authentication plugin class, `com.sun.identity.authentication.spi.JwtReplayPassword`, that uses a JWT-based AES A128CBC-HS256 encryption

algorithm to encrypt the password captured by AM during the authentication process. AM stores the encrypted password in a session property that, later on, IG recovers, decrypts, and replays into legacy applications.

The legacy password replay post-authentication plugin class, `com.sun.identity.authentication.spi.ReplayPasswd`, is deprecated and will be removed in a future release of AM.

To configure password replay for AM and IG, see the *ForgeRock Identity Gateway Gateway Guide*.

For more information about post-authentication plugins, see "Implementing Post-Authentication Plugins" in the *Authentication and Single Sign-On Guide*.

Important

Before configuring the new password replay post-authentication plugin, consider the following points:

- The new password replay post-authentication plugin class is only supported for IG 6 or later. To configure web agents and earlier versions of IG for password replay, use the `com.sun.identity.authentication.spi.ReplayPasswd` class.
- Only one password replay post-authentication plugin class can be active at the same time for an AM deployment.

- **New Monitoring Interfaces**

  AM 6 introduces new monitoring interfaces to expose metrics about the AM installation.

  Additionally, if further analysis and visualization are required, tools such as Grafana can be used to create customized charts and graphs based on the information collected by monitoring.

  The following monitoring interfaces have been added:

  - Prometheus
  - CREST
  - Graphite

  For more information about monitoring services, see "Monitoring Services" in the *Setup and Maintenance Guide*.

- **Proxy Support for ForgeRock's ClientHandler Code**

  AM 6 allows ForgeRock's ClientHandler code, such as the Google reCAPTCHA user self-service feature or AM's social authentication providers, to make requests through the HTTP proxy configured using JVM properties.

  For more information, see "Settings for Configuring a JVM Proxy" in the *Installation Guide*.

- **Amster 6 Released**

  Amster 6 allows you to export and import configurations for AM 6 and later. For more information, see the *ForgeRock Amster Release Notes*.

1.3. Major Improvements

AM 6

- **Authentication Trees**
  - **Audit Logging Added to Authentication Trees**

    AM 6 now logs audit events generated during authentication tree flows. The following events are logged:

    - Reaching a node during the authentication tree flow, and the node's outcome. Audit event: `AM-NODE-LOGIN-COMPLETED`.
    - Completing an authentication tree flow, and the authentication decision. Audit event: `AM-TREE-LOGIN-COMPLETED`.

    To turn off audit logging for authentication trees or nodes, configure the advanced server properties `org.forgerock.openam.auth.audit.nodes.enabled` and `org.forgerock.openam.auth.audit.trees.enabled`. For more information, see "Advanced Properties" in the *Reference*.

- **General**
  - **Support for the `force-change-on-reset` DS Password Policy During User Self-Service Password Reset**

    When the `force-change-on-reset` password policy is configured on a DS user data store, users resetting their passwords using AM's forgotten password feature may be required to reset their passwords twice (prompted by both AM's User Self-Service and DS's password policy).

    AM 6 introduces a new property to the DS user data store, LDAP Proxied Authorization, to support the `force-change-on-reset` password policy.

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

  - **`validate&refresh=false` added to the `sessions` endpoint**

    Validating sessions with the `session?validate` action no longer resets the idle time when called alongside the `refresh=false` action. For example:

```
$ curl \
--request POST
 \
-header "Accept-API-Version: resource=2.1, protocol=1
.0"
--header "iplanetDirectoryPro: AQIC4Dm...NTcy*" \
http://openam.example.com:8080/openam/json/realms/root/sessions?_action=validate&refresh=false
```

This improvement prevents AM from writing to the Core Token Service token store when validating sessions, which is an expensive operation that may not be required on each validation.

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

- **Optimized XUI Delivery Using Webpack**

  AM 6 uses the *Webpack* resource bundler to manage XUI dependencies, optimize deliverables, and package the output.

  ForgeRock provides the source code for the XUI as a Maven project, allowing you to leverage Webpack functionality for customizing the user interface.

  Any existing customizations are not affected and can be applied to AM 6 without modification.

  For more information, see "Customizing the XUI" in the *UI Customization Guide*.

- **Audit Logging Added to User Self-Service**

  AM 6 now logs audit messages generated during the following user self-service events:

  - A user has successfully registered using user self-service. Audit event: `AM-SELFSERVICE-REGISTRATION-COMPLETED`.
  - A user has successfully changed their password using user self-service. Audit event: `AM-SELFSERVICE-PASSWORDCHANGE-COMPLETED`.

- **Stateless OAuth 2.0 Access and Refresh Token Encryption Support**

  AM now supports encryption of stateless OAuth 2.0 access and refresh tokens, to protect the data stored within.

  For more information, see "Configuring Stateless OAuth 2.0 Token Encryption" in the *OAuth 2.0 Guide*.

- **JATO Pages Migrated to XUI**

  In AM 6 the following pages have been migrated into XUI:

  - STS
  - Data Stores

- Agents
- Circles of Trust
- Groups
- Privileges

  This functionality can now be found under Realms > *Realm Name* > Identities > Groups > *Group Name*.

- Identities

  Previously, this page was called Subjects.

- **User Self-Registration Backwards-Compatible Mode Added**

  By default, the user self-registration flow validates the email address after the user has provided their details.

  AM 6 provides a backwards-compatible mode for user self-registration flows configured in OpenAM 13 and 13.5 that allows AM to validate the email address before the user provides their details.

  To activate this mode, enable the Verify Email before User Detail property (Realms > *Realm Name* > Services > User Self-Service > User Registration).

  For more information about the REST implementation, see "Registering Users" in the *User Self-Service Guide*.

1.4. Security Advisories

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

For 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

The following AM software is available on BackStage:

Access Management Software

File	Description
`AM-6.0.0.7.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-6.0.0.7.war`	Deployable web application archive file.
`SSOAdminTools-5.1.1.5.zip`	The .zip file that contains tools to manage AM from the command line.
`SSOConfiguratorTools-5.1.1.5.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 2017.09, Amazon Linux 2

Operating System	Version
SuSE	12
Ubuntu	14.04 LTS, 16.04 LTS
Solaris x64	10, 11
Solaris Sparc	10, 11
Windows Server	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

Web Containers

Web Container[a]	Version
Apache Tomcat	7[b], 8.5, 9
Oracle WebLogic Server	12c
JBoss Enterprise Application Platform	7.1
WildFly AS	10.1, 11
IBM WebSphere	8.5.5.8+, 9

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

[b] 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.

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	6	✔	✔	✔	✔
External Directory Services/ OpenDJ	3.0+	✔	✔	✔	✔
Oracle Unified Directory	11g R2			✔	
Oracle Directory Server Enterprise Edition	11g			✔	
Microsoft Active Directory	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+	Internet Explorer 11+	Edge 25+	Firefox 57+	Safari 11+	Mobile Safari
Windows 8 or later	✔	✔	✔	✔[b]	✔		
Mac OS X 10.11 or later	✔	✔			✔	✔	
Ubuntu 12.04 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] Windows 10 only.

2.7. Supported Upgrade Paths

The following table contains information about the supported upgrade paths to AM 6.0.0.7:

Upgrade Paths

Version	Upgrade Supported?
AM 6.0.x	✔
AM 5.x	✔ [a]
OpenAM 13.x.x	✔
OpenAM 12.0.x	✖

[a]

[a] **Caution**
AM is incompatible with SSO session tokens from OpenAM.
Storage and processing of sessions changed in AM 5: CTS-based (stateful) and client-based (stateless) sessions created by 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 6 software.

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

- 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

AM is incompatible with SSO session tokens from OpenAM.

Storage and processing of sessions changed in AM 5: CTS-based (stateful) and client-based (stateless) sessions created by 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.

AM 6.0.0.7

- LDAPv3Repos LDAP Servers are Now Stored in Comma-Separated Ordered List

  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
```

AM 6

- **Authentication Trees**
  - **Changes to the Zero Page Login and Password Collector Authentication Nodes**

    In AM 5.5.x, the information captured by the Zero Page Login and Password Collector authentication nodes persisted through the lifetime of the authentication tree flow.

    In AM 6, passwords captured by the Zero Page Login and Password Collector authentication nodes are transient. Passwords persist until the authentication flow reaches the next node requiring user interaction.

    This change prevents passwords from being persisted beyond the lifetime of the HTTP request in which they were presented to the AM instance, minimizing the risk of exposing the password to malicious users.

    For more information about authentication nodes, see "Configuring Authentication Nodes" in the *Authentication and Single Sign-On Guide*.

- **General**
  - **Change to the Entropy Bit Length in OAuth 2.0 Access/Refresh Tokens and Authorization Codes**

    The entropy bit length of OAuth 2.0 access/refresh tokens and authorization codes have increased to 160 bits to comply with the recommendation in the OAuth 2.0 RFC.

  - **Changes to the OAuth 2.0 `Token` (`org.forgerock.oauth2.core.Token`) Interface**

    In earlier versions of AM, the methods `getTokenId` and `toMap` contained in the `Token` interface declared that they could throw `ServerException`.

    AM 6 removes the need to catch this exception, which simplifies the usage of the `Token` interface.

You should update any code which uses the `Token` interface to remove the need to catch `ServerException`.

For more information, see the `Token` interface in the *ForgeRock Access Management 6 Public API Javadoc* .

- **Disk Space Requirement Changes**

  DS 6 has increased the threshold for low free space on disk. It now requires free disk space equal to or greater than 5 GB, plus 5% of the total size of the filesystem where DS is installed.

  Therefore, when installing AM to use an embedded DS server as the configuration store, ensure that there is enough free disk space in AM's configuration directory at all times.

- **Naming Convention Changes on Documentation and UI**

  Earlier versions of the AM documentation and the UI classify sessions as *stateful* when AM stores sessions in the CTS token store, and *stateless* when AM returns session state to the client after each request, and require it to be passed in with the subsequent request.

  This naming convention is misleading. The introduction of autonomous session management in AM 5 allows any server on the deployment to satisfy session requests, removing the concept of a home server and therefore, making the Session Service stateless.

  AM 6 removes the stateful/stateless naming convention and classifies sessions depending on where they are stored:

  - CTS-based sessions (previously referred as stateful sessions)
  - Client-based sessions (previously referred as stateless sessions)

- **Enabling SNMP Monitoring in AM**

  Instances of DS 6, including those upgraded from a previous version, require that the `/snmp/opendmk.jar` installer is run, and the resulting library copied to the correct location, to enable SNMP monitoring. The installer is included in the AM 6.0.0.7 ZIP file. Once the installer has been executed, the `jdmkrt.jar` file must be copied from the resulting `/lib` folder to the AM `/WEB-INF/lib` folder.

  For more information, see "SNMP Monitoring" in the *Setup and Maintenance Guide*.

- **Changes to Web Agents and AM Interoperability Requirements**

  AM 6 requires Web Agents 5.x to be in version 5.0.1 or higher. Upgrade any web agent in version 5 before upgrading to AM 6.

- **Changes to Operating System, Client, and Web Container Support**

The tables containing the supported operating system, clients, and web containers have been updated for AM 6.

For more information, see "*Before You Install*".

- **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 migrating to AM 6.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.

- User Self-Service Email Verification Code is One-Time Use

  In previous versions of AM, the password recovery link AM emails to the user when the email verification feature is enabled could be used several times.

  AM 6 whitelists the code contained in the recovery link such that it can only be used once.

4.2. Deprecated Functionality

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

AM 6

- **Password Replay Post-Authentication Class `com.sun.identity.authentication.spi.ReplayPasswd` Deprecated**

  The password replay post-authentication plugin class, `com.sun.identity.authentication.spi.ReplayPasswd`, is deprecated and will be removed in a future release of AM.

  AM 6 includes a new password replay post-authentication class. For more information, see the AM 6 New Features section in the *Release Notes*.

4.3. Removed Functionality

Functionality listed under this section has been removed from AM.

AM 6

- **Agents 2.2 Removed from XUI**

  The XUI pages for the deprecated Agents 2.2 have been removed. Use the **Amster** command to configure or modify Agent 2.2 instances.

Chapter 5

Fixes, Limitations, and Known Issues

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

5.1. Key Fixes

Key Fixes in AM 6.0.0.7

- OPENAM-10127: SessionMonitoringStore should only be instantiated when monitoring is enabled
- OPENAM-11048: OpenAM account lockout does not work when naming attribute and LDAP Users Search Attribute are different
- 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-12965: httpClient not exposed to OIDC Claim Script
- OPENAM-13187: OAuth2 DeviceCode flow does not work with stateless encryption enabled
- OPENAM-13247: Token info endpoint throwing 401
- OPENAM-13268: Initial authz eval request for a given realm takes a long time when there are many policies
- OPENAM-13302: AM Self-registration kba throws an error when a user inputs an answer and presses the enter key.
- OPENAM-13851: Rest STS cannot be created in the Console when upgrading to 6
- OPENAM-13892: Erroneous "Response's InResponseTo attribute is not valid error "SAML2 failover is enabled" when it is not
- OPENAM-13896: Comparison method violates its general contract! seen during amster import
- OPENAM-13991: 'issuer' value in .well-known/openid-configuration response is incorrect for a sub-realm
- OPENAM-14050: LDAP should reestablish connection to the orignal server after it has recovered
- OPENAM-14053: Cannot build openam-ui in Windows for Yarn using mvn

- OPENAM-14080: LDAP Decision Node returns incorrect user attribute to search for in user store
- OPENAM-14147: arg=newsession in XUI does shows just the "Loading..." page
- OPENAM-14174: AM shows Ldapter.delete exception when session expires is triggered
- OPENAM-14189: effectiveRange of Time environment has issue
- 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-14353: Error Message not Displayed when Change Password does not Meet Password Policy
- OPENAM-14369: Upgrading from OpenAM 13.5.0 to AM 6.0.0.x with custom PAPs causes NPE failure
- OPENAM-14393: CTS Operation Fails Entry Already Exists logged for SAML2 Authentication is done
- OPENAM-14427: Certificate Module with option "Match Certificate in LDAP" does not work
- OPENAM-14505: Agent sessions are constrained by Session Quota
- OPENAM-14548: consent page still shows what's been granted/removed as a result of OAuth2 scope policy evaluation
- OPENAM-14573: amlbcookie is not secure when authenticating with trees
- OPENAM-14581: handling ManageNameID fails if NameID does not include SPNameQualifier

Key Fixes in AM 6.0.0.6

- 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-11665: Improve debug logging when unable to login in XUI with users endpoint getting 404 due to KBA attribute issues
- OPENAM-12789: Data store with identities that do not match user search attr cause server error
- OPENAM-13291: Create Identities Page appears broken after upgrade from 5.5 (to 6.0 or 6.5)
- OPENAM-13604: IdP Proxy relays wrong AuthnContextClassRef if the AuthLevel requested by the SP is not 0

- OPENAM-13762: Improve caching of ServiceConfigImpl instances
- OPENAM-13814: User Self Service reCAPTCHA Feature Broken

Key Fixes in AM 6.0.0.5

- OPENAM-8296: OAuth consent screen does not use XUI theme configuration
- OPENAM-11225: idpSingleLogoutRedirect throws 500 error SLO
- OPENAM-13183: Concurrent changePassword requests to the "users" REST endpoint causes "insufficient access rights" failures
- OPENAM-13301: When creating Java/Web agent groups, some properties are not tag-swapped
- OPENAM-13310: Allow id tokens to be issued when no datastore configured
- OPENAM-13315: OIDC no longer supports prompt=consent parameter
- OPENAM-13350: Upgrade from 12.0.x to 6.0.0.2 fails with embedded user store
- OPENAM-13359: P11RSAPrivateKey fails RSA key check.
- OPENAM-13414: Upgrade to AM6 fails if OAuth2 Provider service lacks tokenSigningHmacSharedSecret
- OPENAM-13438: Setting org.forgerock.openam.ldap.heartbeat.timeout=-1 makes AM unusable
- OPENAM-13457: AM 6 XUI favicon icon not being recognised
- OPENAM-13499: Incorrect transaction ID used in access events for CREST endpoints
- OPENAM-13506: OAuth2 Provider Service REST defaultACR input data not validated.
- 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-13577: xmlsec 2.1.1.jar used in AM6 have issues when linebreaks enabled
- OPENAM-13578: KBA are not updatable after upgrade
- OPENAM-13581: "Try Resetting Your Password Again" Link fails if the Single use Token is expired/used
- OPENAM-13649: SuccessUrl redirects not working in Safari
- OPENAM-13670: Selfservice password reset token doesn't work in site due to OPENAM-6426

Key Fixes in AM 6.0.0.4

- OPENAM-10532: SOAPExceptionImpl: Invalid Content-Type:text/html. Is this an error message instead of a SOAP response?
- OPENAM-11407: extra space in the CTS 's connection string " openam.internal.example.com:50389" cause OpenDJ-SDK log to grow
- OPENAM-11642: CustomProperties do not work when creating J2EE/Web Agents via REST
- OPENAM-12173: NumberFormatException for AuthLevel in OAuth2 logs
- OPENAM-12984: Access Token Endpoint issues search request against datastore for OAuth Client
- OPENAM-13031: Failed search for non-existent user in datastore when fetching session properties and user profile is set to ignore
- OPENAM-13085: WSFederation Active Request Profile authentication request hangs on input-less scripted modules
- OPENAM-13128: invalid error message returned when user with expired password authenticates with persistent cookie module
- OPENAM-13236: Amster tries to load custom service subconfiguration before loading realm level configurations
- OPENAM-13245: Omitting Node.Metadata annotation kills the loading of all plugins in AM
- OPENAM-13308: LdapDecisionNode failes when Return UserDN to Datastore is set to false
- OPENAM-13316: LDAP Decision Node does not return Inactive Account result correctly in eDirectory
- OPENAM-13330: Improve SessionResource Authz Module processing
- OPENAM-13347: Inner Tree Node "tree" choice field not populated after upgrade
- OPENAM-13426: EncryptSAMLIDPSPBasicAuthPwdStep fails in upgrade
- OPENAM-13456: AM 6 XUI custom FooterTemplate.html and LoginHeaderTemplate.html not being applied

Key Fixes in AM 6.0.0.3

- OPENAM-10296: Session UI only allows searching for users in datastore
- OPENAM-11240: "Skip This Step" button on the ForgeRock Authenticator (OATH) screen is missing (HOTP)

- OPENAM-11962: Calling Logout and passing a goto URL parameter with an expired session, goto URL is ignored
- OPENAM-12209: 'acr' and 'acr_sig' parameters can become duplicated during step-up authn, should not be present in url
- OPENAM-12338: policies?_action=evaluate checks all policy sets
- OPENAM-13053: ScriptingService doesn't add the new values to whitelist during upgrade
- OPENAM-13078: ScriptedDecisionNode exposes headers in a case sensitive map
- OPENAM-13090: Social Authentication Implementations UI does not accept an auth tree
- OPENAM-13102: Device Match - Server side script fails when error level logging is enabled.
- OPENAM-13138: 500 internal server error if user does not have a session when providing user code in OAuth2 device flow
- OPENAM-13144: DeviceID Profiles are not saved
- OPENAM-13157: DCustom Authentication Nodes not being exported correctly
- OPENAM-13249: AM 6 doesn't recognize custom templates and partials
- OPENAM-13298: OIDC requests with claims request parameter fail

Key Fixes in AM 6.0.0.2

- OPENAM-12419: Policy rules not updated when external configuration store connection restarted
- OPENAM-12784: ProviderConfiguration is not spec compliant
- OPENAM-12867: IdP-Proxy - Single Logout fails as LogoutResponse is not signed
- OPENAM-12912: Upgrade 5.5.x --> 6.x fails if Amster has been used at some point to export/import
- OPENAM-13082: address claim in default OIDC claims script outputs non-spec compliant format
- OPENAM-13083: Profile KBA: custom questions are not displayed
- OPENAM-13100: LDAP Decision node fails with NPE when used with Active Directory

Key Fixes in AM 6.0.0.1

- OPENAM-4040: SSO failure between SPs in separate CoTs with same hosted IDP
- OPENAM-12938: ODSEE fails to load identities

- OPENAM-13006: Missing upgrade steps for OAuth2 ID Token SIgning and Encryption Algorithms
- OPENAM-13008: Occasional shutdown error for AM
- OPENAM-13068: Sample Facebook-ProvisionIDMAccount auth tree has wrong "connections"
- OPENAM-13074: Fix UI sections for authentication modules
- OPENAM-13084: Entity Import ordering in amster
- OPENAM-13099: AM Overview Sample Monitoring Dashboard session metrics also count changes to authentication sessions
- OPENAM-13103: AM Overview Sample Monitoring Dashboard policy throughput metrics not grouped by AM instance

Key Fixes in AM 6

- OPENAM-12703: UnsupportedOperationException seen on SAML related session logout
- OPENAM-12626: OIDC endSession endpoint does not call post authentication plugin onLogout functions
- OPENAM-12553: IdP Logout is ignored when using SAML2 Auth module and trying to use a goto
- OPENAM-12477: id_token requested using grant_type=authorization_code returns auth_time in milliseconds
- OPENAM-12418: Unable to access Forgerock OATH for users with Profile when caching disable
- OPENAM-12415: Self-Service KBA questions of TopLevel Realm(or Global Service) override SubRealm's
- 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-12412: Multi-valued LDAP attributes are not added to the OIDC id_token as expected
- OPENAM-12380: Client ip audit logging is not storing as IP but a list of IPs
- OPENAM-12377: WS-Fed extended metadata with unknown COT value should generate an error
- OPENAM-12370: JWT verification fails when token idle time is too long
- OPENAM-12357: ssoadmin tools distro include release canditate libraries
- OPENAM-12333: AMIdentitySubject policy evaluation not cache when a lot of groups and datatsore is use with delegated admin
- OPENAM-12252: Delegated admin with Stateless Session, causes Admin Console failure.

- OPENAM-12245: "Authentication by Module Instance" policy env condition doesn't work in session upgrade case
- OPENAM-12244: Monitoring services unable to connect to Port
- OPENAM-12234: Values for objects of type com.sun.xml.bind.util.ListImpl are not printed in debug logs
- OPENAM-12226: Device Match - server side script fails
- OPENAM-12219: Resource leak in MonitoringAdapters#getMonAuthList
- OPENAM-12194: SLO with the SAML2 Auth Module PAP redirects to 'XUI/nullnull' when IDP has no SingleLogoutService defined
- OPENAM-12166: Resource #3.0 logoutByHandle request fail with status 500 error
- OPENAM-12161: Expires attribute in WS-Fed Active Requestor Profile is expected but is optional
- OPENAM-12144: getSessionInfo endpoint _fields parameter doesn't work
- OPENAM-12135: OIDC token generated with datastore module takes case from request rather than from the datastore
- OPENAM-12109: Syslog Audit Event Handler buffer size should be configurable
- OPENAM-12082: Outlook with WS-Fed uses cached credential after AD password change.
- OPENAM-12075: OIDC without a datastore returns "User must be authenticated to issue ID tokens"
- OPENAM-12062: XUI DashBoard does not show trusted devices etc if user search attribute of the data store is not 'uid'
- 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-12026: Self-service user registration gets "Bad Request" on LDAP error 19
- OPENAM-12022: Self-service registration for existing user displays "Detected conflict in request"
- OPENAM-12011: Session is not refreshed reliably when using oauth2/authorize endpoint
- OPENAM-11994: NullPointerException in ResourceOwnerOrSuperUserAuthzModule.getUserIdFromUri
- OPENAM-11988: HTTP 500 when validating SSO tokens if API version is omitted in AM 5.5
- OPENAM-11980: Social OIDC wizards do not work when provisioning accounts locally
- OPENAM-11976: XUI Session query session by username does not work with +

- OPENAM-11968: SAML2 Auth Module does not accept SAML2 AuthResponse with no SessionIndex
- OPENAM-11966: saml2 SSO 'better' auth'n comparison fails with 'Invalid status code in response'
- OPENAM-11961: KBA update fails if Self-service is configured in sub-realm and root realm has no datastore
- OPENAM-11956: SAML2 RelayState values are seen as invalid if they are not a URL which appears to go against the spec
- OPENAM-11944: REST OAuth2 creation triggers objectClass=* search
- OPENAM-11937: Federation UI does not allow empty NameIDMappingService
- OPENAM-11925: CORSFIlter causings failures after moving to 5.x from 13.5.x
- OPENAM-11909: Demo user creation is based on whether a userCfg is specified, rather than when it's set to embedded
- OPENAM-11829: SSOToken idletime reset even when it shouldn't be
- OPENAM-11818: Oauth2 authn module incorrectly POST state parameter to token endpoint
- OPENAM-11789: User remains on 'Loading' page with 'OAuth2.0/OIDC' auth module if authId token expires before entering credentials
- OPENAM-11759: Memory leak affecting policy evaluation for stateless sessions
- OPENAM-11746: Syslog data is not fully RFC compliant
- OPENAM-11678: 'Oldest' REST passwordreset selfservice unusable
- OPENAM-11673: Policy evaluation response is incorrect if the URL query string sent for evaluation contains the string ://
- OPENAM-11661: Prevent Restlet from adding the Server header
- OPENAM-11548: Improve Scope validator class loading error handling
- OPENAM-11547: Missing entry or corrupted value in "com.iplanet.am.version" causes upgrade failure
- OPENAM-11491: Upgrading OpenAM results in failure due to restSMS.xml
- OPENAM-11477: SLO through IDP Proxy loses the RelayState
- OPENAM-11432: Extra space in Policy 's Resource Type will cause policy evaluation to fails
- OPENAM-11402: OpenAM does not enforce OAuth2 spec for "Resource Owner Password Credentials Grant" flow

- OPENAM-11398: OpenAM ACI installation instruction does not work for OpenDJ productionMode
- OPENAM-11157: Oauth2/OIDC Authentication redirect goto value wrong when behind reverse proxy
- OPENAM-10673: SAML2 authentication module fails to redirect to IDP after failing DeviceID match module
- OPENAM-10619: Post Authentication Plugin not run during session upgrade
- OPENAM-10591: Generate more debug details about the JSON that is failing when JsonPolicyParser throws a UNABLE_TO_SERIALIZE_OBJECT exception
- OPENAM-9717: TimerPool deadlock on ssoadm shutdown (client SDK)
- OPENAM-9629: OAuth2 flow creates GENERIC CTS tokens that never expire
- OPENAM-8264: Insufficient validator for service property 'iplanet-am-auth-hmac-signing-shared-secret'
- OPENAM-7911: Improve Error Message: "Invalid Suffix"
- OPENAM-5991: IP Address logging in SAML2 audit logs is not consistent
- OPENAM-5865: AuthLevelCondition will not retrieve request auth level for a capital-letter realm.
- OPENAM-1167: WindowsDesktopSSOConfig ClassCastException on saving configuration in admin UI

5.2. Limitations

The following limitations and workarounds apply to AM 6:

- **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>
```

- **OAuth2 Scopes Behavior Affected by Upgrade**

  After an upgrade from OpenAM 12.0.x, OAuth v2.0 scope behavior uses a deprecated implementation class, `org.forgerock.openam.oauth2.provider.impl.ScopeImpl`.

  The workaround is to manually update the OAuth v2.0 providers to use the `org.forgerock.openam.oauth2.OpenAMScopeValidator`.

  For background information, see OPENAM-6319.

- **Supported ID Token Algorithms and Methods not Updated After Upgrade**

  AM 5 added additional algorithms and methods for encrypting ID tokens. Performing an upgrade from OpenAM 13.5 does not add these new values to the affected properties.

After upgrade, navigate to *Realm Name* > Services > OAuth2 Provider > OpenID Connect, and manually update the ID Token Encryption Algorithms supported and ID Token Encryption Methods supported properties.

For more information on the available algorithms and methods, see "Encrypting OpenID Connect ID Tokens" in the *OpenID Connect 1.0 Guide*.

- **Different AM Version Within a Site**

  Do not run different versions of AM together in the same AM site.

- **Avoid use of Special Characters in Policy or Application Creation**

  Do not use special characters within policy, application or referral names (for example, "my +referral") using the Policy Editor or REST endpoints as AM returns a 400 Bad Request error. The special characters are: double quotes ("), plus sign (+), command (,), less than (<), equals (=), greater than (>), backslash (\), and null (\u0000). (OPENAM-5262)

- **XACML Policy Import and Export**

  AM can only import XACML 3.0 files that were either created by an AM instance, or that have had minor manual modifications, due to the reuse of some XACML 3.0 parameters for non-standard information.

- **Custom Profile Attributes Are Not Visible in the User Profile Only With the XUI**

  Custom profile attributes do not appear in the user profile when users log in to AM using the XUI.

5.3. Known Issues

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

Known Issues in AM 6.0.0.7

- OPENAM-4713: Can't use Common Tasks wizards when logged in as a delegated administrator
- OPENAM-9777: Json Web Key URI in OAuth2 OpenID connect client config pre-populated incorrectly
- OPENAM-10377: Agent creates unexpired tokens which are not deleted from CTS
- OPENAM-12508: import-entity for SAML remote SP does not work anymore
- OPENAM-14146: administrative authentication is not triggered for XUI-based console
- OPENAM-14207: NullPointerException AM Console if IDPSSODescriptor is missing attribute 'WantAuthnRequestsSigned'

- OPENAM-14215: Automatic login fails after Self Registration with Authentication Trees
- OPENAM-14229: custom AuthorizeTemplate under theme not used
- OPENAM-14234: NullPointerException in SP-initaited SSO if IDPSSODescriptor is missing attribute 'WantAuthnRequestsSigned'
- OPENAM-14240: FMSigProvider.verify does not tell if certificates are provided
- OPENAM-14245: Console error when adding entity to circle of trust
- OPENAM-14277: IdP-Proxy - SP part prompts for authentication if no local user can be found
- OPENAM-14290: Caching issue for 'users' REST endpoint
- OPENAM-14309: Import of SAML2 Metadata not signed on EntityDescriptor fails.
- OPENAM-14343: AM console - localisation issue for algorithms in global Common Federation Configuration
- OPENAM-14499: SAML IdP-initiated SSO without existing SSO Session - value of 'goto' parameter not URLencoded
- OPENAM-14500: SAML SP-initiated SSO without existing SSO Session - value of 'goto' parameter not URLencoded
- OPENAM-14576: Configuration LDAP accessed when users endpoint accessed
- OPENAM-14580: IdP-initiated ManageNameID request fails with "unsuported binding" when IdP meta alias is incorrect.
- OPENAM-14594: Possible thread-safety issue in OIDC pairwise subject identifiers
- OPENAM-14624: XUI fails to load partial potential issue with webpacks
- OPENAM-14755: NullPointerException if auth module callback xml file can not be retrieved by ResourceLookup
- OPENAM-14782: AuthTree created Session does not use per User Session Service settings
- OPENAM-14808: "User name/password combination is invalid." error message shown when provided with incorrect cookie domain
- OPENAM-14848: Insufficient debug logging in OpenID Connect authentication module
- OPENAM-14849: Insufficient debug logging in Scripted authentication module

Known Issues in AM 6.0.0.6

- OPENAM-5867: Data Store LDAP server (admin-ordered) list is reordered by OpenAM

- OPENAM-13720: Public API method LDAPUtils.convertToLDAPURLs can not handle IPv6 literals
- OPENAM-13740: File descriptor / Connection leak when LDAP connection handshake fails/times out
- OPENAM-13856: Activity audit events are logged for authentication sessions
- OPENAM-13860: REST API "PUT /global-config/realms/{realmref}" broken
- OPENAM-13890: Install.log logs AMLDAPUSERPASSWD in plaintext
- OPENAM-13892: Erroneous "Response's InResponseTo attribute is not valid error SAML2 failover is enabled" when is is not
- OPENAM-13899: XUI - USS - Forgotten Password flow without KBA ends up in a loop
- OPENAM-13904: Authentication via REST API - Switching realms is not possible
- OPENAM-13905: XUI Authentication - Switching realms is not possible
- OPENAM-13934: saml2error.jsp fails with exception when malformed SAML2 response given
- OPENAM-13940: Session quota limits not applied when using trees
- OPENAM-13978: Session Upgrade - AuthLevel format changes

Chapter 6
Documentation Updates

The following table tracks changes to the documentation set following the release of AM 6:

Documentation Change Log

Date	Description
	Release of the AM 6.0.0.7 patch bundle release. The following documentation changes were made: • Added some caveats to setting up SAML v2.0 realms configured for client-based sessions. For more information, see "SAML v2.0 and Session State" in the *SAML v2.0 Guide*. • Added text to the LDAP People Container Value property, `sun-idrepo-ldapv3-config-people-container-value`. For more information, see "Active Directory Configuration Properties" in the *Setup and Maintenance Guide*. • Added clarification for the `Auth URL` property in the SAMP IdP configuration. For some information, see Local Configuration in the *SAML v2.0 Guide*. • Added suggestions for configuring keystores. For more information, see "Introducing Keystores" in the *Setup and Maintenance Guide*. • Removed deprecated JVM option, `-XX:+UseCMSCompactAtFullCollection`. For more information, see "Tuning Java Virtual Machine Settings" in the *Installation Guide*. • Expanded text on saved OAuth 2.0 consent. For more information, see "Managing OAuth 2.0 Consent" in the *OAuth 2.0 Guide*. • Added missing information for the User Self-Service Forgotten Password feature. For more information, see "To Configure User Self-Registration by AM" in the *User Self-Service Guide*. • Added text to check the process limits using **ulimit -u**. For more information, see "Setting Maximum File Descriptors and Processes Per User" in the *Installation Guide*. • Added an important admonition that if AM cannot access the CTS token store, users wlll not be able to log in. For more information, see "CTS Configuration" in the *Installation Guide*.

Date	Description
	• Corrected the **ssoadm** version to 5.1.1.5. For more information, see "Files to Download". Added a release note to the 6 release, `User Self-Service Email Verification Code is One-Time Use`.
2018-11-22	Release of the AM 6.0.0.6 patch bundle release.
2018-10-22	Release of the AM 6.0.0.5 patch bundle release.
2018-08-24	Release of the AM 6.0.0.4 patch bundle release. The following documentation updates were made: • Added a note on how the update process must be able to unlock the `keystore.jceks` file. For more information, see "Keystore Configuration After Upgrade" in the *Setup and Maintenance Guide*. • Added a section on performing session upgrade. For more information, see "Performing Session Upgrade" in the *Authentication and Single Sign-On Guide*. • Fixed an error in step 4 under the instructions for how to enable SNMP monitoring. For more information, see "SNMP Monitoring" in the *Setup and Maintenance Guide*.
2018-07-27	Release of the AM 6.0.0.3 patch bundle release. Added a note about the increase in the entropy of stateful OAuth 2.0 access/refresh tokens and authorization codes. For more information, see AM 6.
2018-06-15	Release of the AM 6.0.0.2 patch bundle release.
2018-05-25	Release of the AM 6.0.0.1 patch bundle release. Added a note on how account lockout settings only apply to authentication modules and chains. For more information, see "*Implementing Account Lockout*" in the *Authentication and Single Sign-On Guide*. Added information on the supported LDAP types and operations for Sun/Oracle DSEE. For more information, see "Sun/Oracle DSEE Configuration Properties" in the *Setup and Maintenance Guide*.
2018-05-13	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	Initial release of AM 6.0.

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, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.