Release Notes

/ ForgeRock Access Management 7.0.1

Latest update: 7.0.1

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 (AM). ForgeRock Access Management provides intelligent authentication, authorization, federation, and single sign-on functionality.

Table of Contents

Overview

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.

Patch Releases

ForgeRock periodically issues patch releases with important fixes to bugs. Patch releases focus solely on fixing existing bugs, and improve the functionality, performance, and security of your deployment.

The patch can be deployed as an initial deployment or used to upgrade from an existing version (see "*Supported Upgrade Paths*" in the *Upgrade Guide*).

- **AM 7.0.1** is the latest release targeted for AM 7 deployments and can be downloaded from the *ForgeRock Backstage* website.

New Features

What's New in AM 7.0.1

- No new features have been added in this release.

What's New in AM 7

ForgeRock Access Management 7 is a major release that introduces new features, functional enhancements, and fixes.

- Added OAuth 2.0 Mutual TLS (mTLS) Support

  AM 7 adds support for draft 12 of the OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens specification, a key component of ForgeRock's Open Banking and Revised Payment Services Directive (PSD2) support.

  For information about authenticating an OAuth 2.0 client using mTLS certificates, see "Authenticating Clients Using Mutual TLS" in the *OAuth 2.0 Guide*.

  For information about issuing certificate-bound OAuth 2.0 access tokens, see "Certificate-Bound Proof-of-Possession" in the *OAuth 2.0 Guide*.

- Added OAuth 2.0 Access Token Modification Scripts

  AM 7 adds support for scripting the modification of issued OAuth 2.0 access tokens. You can add properties to the access token, for example values taken from the resource owner's profile such as telephone number or email address.

  For information, see "*Modifying the Content of Access Tokens*" in the *OAuth 2.0 Guide*.

- Added OpenID Connect Authentication Node

  AM 7 introduces an OpenID Connect authentication node, for authenticating users from an OpenID Connect-compliant identity provider.

  For more information about the OpenID Connect authentication node, see OpenID Connect Node

- Added OpenID Connect Client Initiated Backchannel Authentication (CIBA) Support

  AM 7 introduces support for CIBA, which allows a client application, known as the *consumption device*, to obtain authentication, and consent from a user without requiring the user to interact with it directly.

  Instead, the user authenticates and consents to the operation using a separate, "decoupled" device, known as the *authentication device*. For example, an authenticator application, or a mobile banking application on their mobile phone.

  For more information, see "Backchannel Request Grant" in the *OpenID Connect 1.0 Guide*

- New Extension Point to Customize Public Key ID (`kid`)

  By default, AM generates a key ID (`kid`) for each public key exposed in the `jwk_uri` URI when AM is configured as an OAuth 2.0 authorization server.

  AM 7 introduces a new extension point, `KeyStoreKeyIdProvider`, to customize the key ID values associated with public keys stored in keystore secret stores.

  For more information, see "Customizing Public Key IDs" in the *OpenID Connect 1.0 Guide*.

- SAML v2.0 Changes and Improvements

  AM 7 introduces a new user interface for managing SAML v2.0 entities, and circles of trust. For more details, see "*Configuring IDPs, SPs, and CoTs*" in the *SAML v2.0 Guide*.

  The UI is backed by new `/federation` and `/saml2` REST endpoints, for programmatically creating and managing SAML v2.0 deployments. The endpoints are documented in the "*REST API Explorer*" in the *Getting Started with REST*.

  The new UI supports SAML v2.0 IDP and SP entities only. After upgrade, entities that do not have IDP or SP roles will be listed, but cannot be inspected or edited using the UI. An error will display in the UI when trying to access these entities.

  Entities containing roles other than IDP and/or SP will only display the IDP and/or SP roles.

In addition, SAML v2.0 signing and encryption now uses AM's secret stores functionality. AM upgrades SAML v2.0 Service Configurations from previous versions to use secret stores in AM 7. The service itself is no longer required, and is deleted by the upgrade process once the configuration has been migrated. The global service still remains, though.

For more details, see "*Signing and Encryption*" in the *SAML v2.0 Guide*.

As part of this change, the way metadata is stored and generated by AM has changed. For example:

- Encryption algorithms in the standard metadata are now part of the extended metadata.
- Key descriptor elements have been removed from the standard metadata.
- Attributes related to signing and encryption have been removed from the extended metadata.
- The `Secret ID Identifier` property has been added to the extended metadata.

The exported metadata remains unchanged. You do not need to share the metadata of your providers again due to the changes previously explained.

Moreover, as part of hardening the security around the SAML v2.0 implementation, the URLs specified in the Assertion Consumer Service must exactly match the SP's scheme, FQDN, and port.

If the URL does not match, the SAML v2.0 flow will fail and AM will log `Invalid Assertion Consumer Location specified` in the audit log file.

- New REST-based Method for Configuring CORS Support

  AM 7 introduces a new REST endpoint, `/global-config/services/CorsService`, for configuring how to handle cross-origin resource sharing (CORS).

  Clients and applications can use the endpoints to configure their own CORS requirements, without having to restart AM or the container in which it runs.

  For more information, see "Configuring CORS Support" in the *Security Guide*.

- Added Suspended Authentication Support

  AM 7 introduces support for suspending an authentication tree, and saving any input made so far. The user is sent a URL, sometimes referred to as a *magic link*, which lets them resume from where they left off, perhaps after closing the browser, in a different browser, or even on a different device.

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

- **Added SameSite Cookie Support**

  AM 7 adds support for applying *SameSite* cookie rules, as per internet-draft Cookies: HTTP State Management Mechanism.

For more information, see "*Securing Network Communication*" in the *Security Guide*.

As part of this change, AM 7 also introduces a filter in its application description file (`web.xml`) that sets the `Secure` flag on the cookies AM produces if any of the following is true:

- The request comes in through a connection marked as secure. For example, because you have marked an HTTP connector as secure in Tomcat.
- The request comes in through an HTTPS connector.

Automatically promoting cookies to secure ensures that the functionality continues to work with the `SameSite` changes, because you can only opt out of `SameSite` if a cookie is marked as secure.

To ensure that non-secure requests are load-balanced correctly, the `amlbcookie` cookie is already excluded by default. If you are using a custom cookie for sticky load balancing, you may want to add it to the list of excluded cookies.

For more information, see "Managing the Secure Cookie Filter" in the *Security Guide*.

- Added Identity Gateway Agents

  AM 7 adds support for creating Identity Gateway Agents, which configure credentials used by Identity Gateway when making policy evaluation calls, and when registering to receive session and policy configuration notifications over the Web Sockets protocol.

  For more information, see Setting Up AM in the *IG Gateway Guide*.

- Added Failover and Affinity Support to External Policy and Application Stores

  AM 7 adds support for both failover and affinity deployments of external policy and application stores. Previously you could only specify a single directory server instance, making it a single point of failure.

  For information, see "Setting Up Policy and Application Stores." in the *Setup Guide*.

- OAuth 2.0 Dynamic Client Registration Management Protocol (RFC7592) Fully Supported

  AM 7 adds support for OAuth 2.0/OpenID Connect clients to edit and delete their client profile data as per RFC7592.

  Earlier versions of AM offered support for read operations only.

  For more information, see "Dynamic Client Registration Management" in the *OpenID Connect 1.0 Guide*.

- Added Support for the `id_token_hint` Parameter on the OAuth 2.0/OpenID Connect Authorization Endpoint

AM 7 adds support for client relying parties to use the `id_token_hint` parameter in their request to the authorization endpoint as a hint about the end user's session. AM uses the ID token to verify whether the end user specified on it has a valid session in AM.

As part of this change, the authorization endpoint supports the new `none` response type.

For more information, see "/oauth2/authorize" in the *OAuth 2.0 Guide* and "Retrieving Session State without the Check Session Endpoint" in the *OpenID Connect 1.0 Guide*.

- Added Support for Debug Logging with Logback

  AM 7 adds support for configuring debug logging by using Logback.

  Functionality provided by Logback can now easily be applied to the debug logging output of AM, for example log file rotation, and file compression.

  For more information, see "*Debug Logging*" in the *Maintenance Guide*.

- Added Support for the JWT Profile for OAuth 2.0 Authorization Grant

  AM 7 adds support for the JWT profile for OAuth 2.0 Authorization Grant, defined in the *RPC 7523* specification.

  As part of this feature, AM includes a new agent of the type Trusted JWT Issuer.

  For more information, see "JWT Profile for OAuth 2.0 Authorization Grant" in the *OAuth 2.0 Guide*.

- Added Support for Wildcards in OAuth 2.0 Redirection URI Ports

  AM 7 allows the use of wildcards (*) in the redirection URI port to match one or more ports.

  This feature requires that the URL configured in the redirection URI is either `localhost`, `127.0.0.1`, or `::1`. For example, `http://localhost:*/`, `https://127.0.0.1:80*/`, or `http://[::1]:*`.

  For more information, see the Allow wildcard ports in redirection URIs property in Core Properties in the *OAuth 2.0 Guide*.

- Added Support for the JWT Response for OAuth Token Introspection Internet Draft

  AM 7 adds support for clients to configure whether the token introspection endpoint should return its response in JSON format or as a JWT, as per the JWT Response for OAuth Token Introspection Internet Draft.

  This new feature includes a new drop-down menu to choose the endpoint's output format, as well as several new parameters to configure whether the JWT should be signed, or signed and encrypted.

  By default, even after an upgrade, clients are configured to receive the output in JSON format.

  For more information, see "/oauth2/introspect" in the *OAuth 2.0 Guide*.

- Added New Session Property Whitelist Setting

  AM 7 introduces a new session property whitelist setting, `Session Properties to return for session queries`.

  This setting shows a list of properties that can be returned to admins in a REST session query response.

  For more information about the session property whitelist settings, see "Session Property Whitelist Service" in the *Reference*.

- Added Support for Macaroons

  AM 7 adds support for a new token format called Macaroons, which can be used when issuing OAuth 2.0 access and refresh tokens.

  Macaroons allow caveats to be appended to them, which restrict how a token can be used. Macaroons provide additional security, as tokens can be restricted just before use. For example, you can add a 5-second expiry time to a macaroon access token before sending it to an API, or bind it to a TLS client certificate before use.

  As part of this change, AM has added a new endpoint which can be used to inspect and manipulate macaroons. This endpoint is available under `/json/tokens/macaroon`.

  For more information, see "*Macaroons as Access and Refresh Tokens*" in the *OAuth 2.0 Guide*.

- Added New Common Federation Configuration Settings

  AM 7 introduces the following Common Federation Configuration settings:

  - `AES Key Wrap Algorithm`, which enables you to set which AES key wrap algorithm to use when the remote entity provider does not specify which key wrap algorithm it supports.
  - `RSA Key Transport Algorithm`, which enables you to set which RSA key transport algorithm to use when the remote entity provider does not specify which key transport algorithm it supports.

  For more information about the Common Federation Configuration settings, see "Common Federation Configuration" in the *Reference*.

- New Device Nodes Added for Forgerock SDK Support

  AM 7 introduces a number of new nodes for profiling devices when using the ForgeRock SDKs:

  Capture

  - "Device Profile Collector" in the *Authentication and Single Sign-On Guide*

  Store

  - "Device Profile Save" in the *Authentication and Single Sign-On Guide*

Compare

- "Device Match" in the *Authentication and Single Sign-On Guide*
- "Device Profile Location Match" in the *Authentication and Single Sign-On Guide*
- "Device Geofencing" in the *Authentication and Single Sign-On Guide*
- "Device Tampering Verification" in the *Authentication and Single Sign-On Guide*

- New Authentication Nodes Added

  AM 7 introduces the following authentication nodes:

Node	Description
"Anonymous Session Upgrade Node"	Lets anonymous users upgrade their session to a non-anonymous one.
"Kerberos Node"	Enables Window desktop single sign-on such that a user who has already authenticated with a Kerberos Key Distribution Center can authenticate to AM without having to provide the login information again.
"SAML2 Authentication Node"	(Previously in Marketplace) Lets you integrate SAML v2.0 SSO into an AM authentication tree. Use it when deploying SAML v2.0 single sign-on in integrated mode (SP-initiated SSO only).
"Write Federation Information Node" in the *Authentication and Single Sign-On Guide*	(Previously in Marketplace) Creates a persistent link between a remote IdP account and a local account in the SP, if none exists yet. If a transient link exists, it is persisted. Existing account links with different IdPs are not lost.
"CAPTCHA Node" in the *Authentication and Single Sign-On Guide*	Implements Google's and hCaptcha's CAPTCHA widgets.
"WebAuthn Device Storage Node" in the *Authentication and Single Sign-On Guide*	Lets you save FIDO2 device data to a profile after having first captured and analyzed the information; for example, with a Scripted Decision node.
"Certificate Collector Node" in the *Authentication and Single Sign-On Guide*	(Previously in Marketplace) Collects an X.509 digital certificate from the user that is authenticating, so that AM can use it in place of other types of credentials.
"Certificate Validation Node" in the *Authentication and Single Sign-On Guide*	(Previously in Marketplace) Validates a digital X.509 certificate collected by the "Certificate Collector Node" in the *Authentication and Single Sign-On Guide*.
"Certificate User Extractor Node" in the *Authentication and Single Sign-On Guide*	(Previously in Marketplace) Extracts a value from the certificate collected by the "Certificate Collector Node" in the *Authentication and Single Sign-On Guide*, and searches for it in the identity store.

Node	Description
"Authenticate Thing Node" in the *Authentication and Single Sign-On Guide*	Authenticates an IoT thing.
"Register Thing Node" in the *Authentication and Single Sign-On Guide*	Registers an IoT thing.

- Added Local Storage Support for SAML v2.0 Single Sign-on

  AM 7 stores SAML v2.0 single sign-on progress as client-side data when using web browsers that support local storage, removing the need to use sticky load balancing.

  For more information, see "Session State Considerations" in the *SAML v2.0 Guide*.

- Added Endpoint to Get Session Information and Also Reset Idle Timeout

  AM 7 includes a new `getSessionInfoAndResetIdleTime` endpoint that resets the idle timeout when obtaining information about a session. The existing `getSessionInfo` endpoint does not reset the idle timeout.

  For more information, see "Obtaining Information About Sessions Using REST" in the *Sessions Guide*.

- Added a DevOps-friendly Way of Changing the Password of the `amAdmin` User

  AM 7 includes a DevOps-friendly way of changing the password of the `amAdmin` user based on the secret stores API.

  For more information, see "Changing the amAdmin Password (Secret Stores)" in the *Security Guide*.

- Added Recursive OAuth 2.0 Introspection Scope

  AM 7 adds the `am-introspect-all-tokens-any-realm` scope, which lets a client introspect tokens issued to other clients, as long as they are registered in the realm of the introspecting client, or in a subrealm of it.

  For more information, see "Special Scopes" in the *OAuth 2.0 Guide*.

- New Method to Retrieve Data from Authentication Trees' Shared State

  AM 7 introduces a new tree shared state called the *secure state*. In cases where a node needs to process sensitive information later on in the authentication flow, AM promotes the data stored in the `transientState` object to the `secureState` object and encrypts it with the key stored in the new `am.authn.trees.transientstate.encryption` secret ID.

  What is affected by this new feature?

- The introduction of the `am.authn.trees.transientstate.encryption` secret ID requires that you make available an AES 256-bit key called `directenctest` to your environment **before upgrading to AM 7**, if one is not already available.

  Failure to do so will result in AM not starting up after upgrade, and the following error will show in the logs:

  ```
  Unknown key aliases in configuration: directenctest
  ```

  For more information, see "*Upgrading AM Instances*" in the *Upgrade Guide*.

  On new installations, ensure that you change the default alias mapped to this secret ID, and that it is always mapped to an existing, resolvable secret. Failure to do so may result in trees not working as expected.

- The introduction of this new state has changed the way you should retrieve data from the shared state when coding your authentication nodes. Instead of using the `context.sharedState.get()` or `context.transientState.get()` methods, use the `context.getState()` method.

  For a given variable, the `context.getState()` method tries to retrieve data from the different states in the following order:

  1. sharedState
  2. transientState
  3. secureState

  This change also affects Scripted Decision Node scripts.

  For more information, see "Storing Values in Shared Tree State" in the *Authentication Node Development Guide*.

- New Google KMS Secret Store

  AM 7 lets you map secrets retrieved from the Google Cloud Key Management Service (KMS) for any feature in AM that supports secret stores.

  Support includes:

  - Mapping Google Cloud KMS secrets to secret IDs used for signing and verification purposes. Using Google Cloud KMS secrets as mappings for encryption and decryption secret IDs is *not* supported.
  - Using a Google Cloud KMS secret to decrypt secrets loaded using other secret stores, or to decrypt the hashed password of the `amAdmin` user.

  For more information, see "Google KMS Secret Stores" in the *Security Guide*.

- Added ForgeRock Go Usernameless Web Authentication

With ForgeRock Go, you can create a secure and seamless login experience by authenticating with any credential on the user's device that supports FIDO2 WebAuthn.

You can also extend passwordless authentication to include usernameless authentication with popular authenticators that support resident keys; for example, Windows Hello (biometric authenticators).

For information, see "Configuring Usernameless Authentication with ForgeRock Go" in the *Authentication and Single Sign-On Guide*.

- Added Support for Web Authentication Trust Anchors and TPM

  AM 7 adds support for verifying the attestation data provided by FIDO2 devices against certificate chains issued by the device vendor.

  The TM attestation format is now supported.

  You can also enable revocation checking, if the certificate chains contain CRL or OCSP entries.

  For information, see "Configuring WebAuthn Trust Anchors" in the *Authentication and Single Sign-On Guide*.

- New Account Active Check Authentication Module

  AM 7 includes a new Account Active Check authentication module, which lets you determine whether an account is marked as active, or locked, without having to run through the remainder of the authentication chain.

  For more details, see "Account Active Check Module" in the *Authentication and Single Sign-On Guide*.

Major Improvements

Improvements in AM 7.0.1

- No major improvements have been added in this release.

Improvements in AM 7

- **OAuth 2.0/OpenID Connect 1.0**
  - **Authentication Trees Supported as Authentication Method for Resource Owner Password Credentials Flow**

    In earlier versions of AM, only authentication chains could be used to authenticate the credentials of a user during the resource owner password credentials OAuth 2.0 grant flow.

In AM 7, you can use either a tree or a chain to authenticate a resource owners' credentials.

You can specify the chain or tree by using any of the following methods:

- Globally, for all realms, by navigating to Configure > Authentication > Core Attributes > Core, and setting the Organization Authentication Configuration property.
- Individually for a realm, by navigating to Realms > *Realm Name* > Authentication > Settings > Core, and setting the Organization Authentication Configuration property.
- Individually for a realm, overriding the realm-level setting above, by navigating to Realms > *Realm Name* > Services > OAuth2 Provider > Advanced, and setting the Password Grant Authentication Service property.
- For a specific access token REST request, by setting the `auth_chain` parameter.

For more information, see "Resource Owner Password Credentials Grant" in the *OAuth 2.0 Guide*.

- Client Certificate Revocation Check Added for OAuth 2.0 Mutual TLS Client Authentication

  AM 7 adds new settings to check whether client certificates have been revoked when mutual TLS is configured as an OAuth 2.0 client authentication method.

  For more information, see "Mutual TLS Using Public Key Infrastructure" in the *OAuth 2.0 Guide*.

- Additional Trusted Header Formats Added for OAuth 2.0 Mutual TLS Client Authentication

  Earlier versions of AM supported receiving client certificates in *raw* PEM-encoded format for OAuth 2.0 mutual TLS, when SSL is terminated at a reverse proxy or load balancer.

  AM 7 adds support for receiving PEM-encoded certificates in the following formats:

  - URL-encoded, for compatibility with the NGINX `$ssl_client_escaped_cert` variable.
  - URL-encoded, and included as one field in a multi-field header, for compatibility with the Envoy `x-forwarded-client-cert` header.

  The Certificate authentication module now also supports PEM-encoded certificates that are also URL-encoded for compatibility with NGINX. The multi-header format of the Envoy headers are not supported by the module.

  For more information, see "Providing Client Certificates to AM" in the *OAuth 2.0 Guide*.

- Authentication Nodes Reorganized into Categories and Filtering Support Added

  The number of authentication nodes available for creating intelligent authentication trees in AM 7 has increased considerably. To aid in creating authentication trees, authentication nodes are now organized into categories. Also, each node has a number of tags used for filtering, including synonyms and other keywords to help locating the correct node for the job.

When creating your own nodes, you can add tags to the meta data to include them in an existing category, and to help administrators locate your node.

For more information, see "To Create an Authentication Tree" in the *Authentication and Single Sign-On Guide* and "The Meta Data Annotation" in the *Authentication Node Development Guide*.

- Transactional Authorization Can Return HTTP 401 Messages on Authentication Failure

  In earlier versions of AM, a transactional authorization advice that failed due to invalid credentials always returned an HTTP 200 message.

  Then, the user would be redirected to the protected resource, where policy evaluation would fail.

  AM 7 introduces a new advanced server property to control whether transactional authorization should return an HTTP 200 or an HTTP 401 message depending on the needs of your environment.

  In both cases, users cannot access the protected resources when they fail to complete the required actions during transactional authorization.

  For more information, see the `org.forgerock.openam.auth.transactionauth.returnErrorOnAuthFailure` advanced server property.

- Custom Authentication Nodes Can Set Custom Error Messages Returned on Authentication Failure

  A new `errorMessage` property has been added to the `Action` interface. The property allows a custom error string to be set, or updated, by a node. The error message is included in the JSON response sent when an authentication tree reaches the *Failure* node.

  For more information, see "The Action Interface" in the *Authentication Node Development Guide*.

- Scripted Authentication Nodes Can Access Additional Functionality

  AM 7 adds support for the scripted authentication node to use callbacks, and additional features, such as access to `transientState`.

  For more information, see "Scripted Decision Node API Functionality" in the *Authentication and Single Sign-On Guide*.

- Relaxed Restrictions for SAML v2.0 with Client-based Sessions

  The restriction against implementing SAML v2.0 single sign-on (SSO) and single logout (SLO) when running AM with client-based sessions has been updated. For more information, see "Session State Considerations" in the *SAML v2.0 Guide*.

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

  AM 7 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 Guide*.

- JMS Audit Logging Batch Configuration has Changed

  The `batch` configuration for the JMS audit handler has changed to support reconnection if the broker becomes unavailable.

  This change renames the `batch.pollTimeoutSec` setting to `batch.writeInterval` setting. It removes the following settings:

  - `batch.batchEnabled`
  - `batch.insertTimeoutSec`
  - `batch.shutdownTimeoutSec`
  - `batch.threadCount`

  For more information, see "*Setting Up Audit Logging*" in the *Security Guide*.

- New LDAP Decision Node Outcome

  AM 7 includes a new `Cancelled` outcome for the LDAP Decision Node.

  If a password policy forces a user to change their password on first login when using the LDAP Decision Node, the user is sent to a password change screen where they must enter their current password, new password, and new password confirmation. If the user cancels this form, the tree evaluation continues along the `Cancelled` outcome path and the authentication will fail.

  For more information, see "LDAP Decision Node" in the *Authentication and Single Sign-On Guide*.

- Delegated Administrators Have Read-Only Access to Other User's Devices

  AM 7 adds support for delegated administrators to have read access to other user's device details, by using the `devices` REST endpoint.

  For information on delegating admin access, see "To Delegate Privileges" in the *Security Guide*.

- Improvements to the CORS Service

  AM 7 adds a user interface to the existing REST interface for configuring CORS configurations.

  You can also now add JavaScript origins directly in OAuth 2.0 clients, rather than having to manually add CORS configuration for them.

For more information, see "Configuring CORS Support" in the *Security Guide*.

- Improvements for Registering ID Repo Plugins by Using Annotations

  AM 7 includes a new method for registering your custom ID repo plugins, without having to use the **ssoadm** command.

  For more information on the new `@IdRepoConfig` annotation, see "Identity Repository Plugin Deployment" in the *Setup Guide*.

- Scripted Decision Nodes Can Now Access the Identity Store

  AM 7 improves the scripted decision node by giving it access to the identity store.

  Now you can look up profile attributes and use them elsewhere in your authentication trees.

  For more details, see "Scripted Decision Node API Functionality" in the *Authentication and Single Sign-On Guide*.

- New External Login Page URL Property

  AM 7 includes a new External Login Page URL property in the Authentication Service. It specifies the URL of the external login user interface, if the authentication user interface is hosted separately from AM.

  You can specify the external login page URL by using either of the following methods:

  - Globally, for all realms, by navigating to Configure > Authentication > Core Attributes > General, and setting the External Login Page URL property.
  - Individually for a realm, by navigating to Realms > *Realm Name* > Authentication > Settings > General, and setting the External Login Page URL property.

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

- Changes to Web and Java Agents Profiles

  - Several properties that used to be configured as custom properties (`com.sun.identity.agents.config.freeformproperties`) have been added as regular properties.

    During upgrade, the process checks the custom properties configured for each agent profile and converts the properties to their regular counterparts, as appropriate.

    Avoid configuring properties twice. Java Agents of any version and Web Agents 5.6.3 or later honor the configuration of the advanced properties over that of the regular properties.

    Caution

    (Web Agents earlier than 5.6.3) Upgrading to AM 7 will overwrite the value of the original custom properties with the default value of the new UI properties.

To work around this issue, perform one of the following actions:

- Upgrade to Web Agents 5.6.3 or later before upgrading to AM 7.
- After upgrading to AM 7, reconfigure the properties that you configured as custom properties in their new UI counterparts.

- Several deprecated properties have been removed from the profile:

  + *Properties Removed from Java Agents*

```
com.sun.identity.client.notification.url
com.sun.identity.agents.config.remote.logfile
com.sun.identity.agents.config.logout.handler
com.sun.identity.agents.config.shortened.privileged.attribute
com.sun.identity.agents.config.verification.handler
com.sun.identity.agents.config.privileged.attribute.mapping.enable
com.sun.identity.agents.config.privileged.session.attribute
com.sun.identity.agents.config.auth.handler
com.sun.identity.agents.config.default.privileged.attribute
com.sun.identity.agents.config.privileged.attribute.type
com.sun.identity.agents.config.privileged.attribute.tolowercase
com.sun.identity.agents.config.privileged.attribute.mapping
com.sun.identity.agents.config.login.use.internal
com.sun.identity.agents.config.login.error.uri
com.sun.identity.agents.config.logout.application.handler
com.sun.identity.agents.config.notenforced.refresh.session.idletime
com.sun.identity.agents.config.login.content.file
com.sun.identity.agents.config.cdsso.clock.skew
com.sun.identity.agents.config.cdsso.trusted.id.provider
com.sun.identity.agents.config.cdsso.cdcservlet.url
com.iplanet.am.cookie.name
com.sun.identity.agents.config.amsso.cache.enable
com.sun.identity.agents.config.cdsso.enable
com.iplanet.am.session.client.polling.period
com.sun.identity.policy.client.booleanActionValues
com.sun.identity.agents.config.login.url.prioritized
com.sun.identity.agents.config.login.url.probe.timeout
com.sun.identity.policy.client.cacheMode
com.sun.identity.agents.config.logout.url
com.sun.identity.agents.config.logout.url.prioritized
com.sun.identity.agents.config.logout.url.probe.timeout
com.sun.identity.agents.config.logout.url.probe.enabled
com.sun.identity.agents.config.login.url.probe.enabled
com.sun.identity.idm.remote.notification.enabled
com.sun.identity.sm.cacheTime
com.sun.identity.sm.notification.enabled
com.sun.identity.policy.client.clockSkew
com.iplanet.am.sdk.remote.pollingTime
com.sun.identity.agents.config.bypass.principal
com.iplanet.security.encryptor
com.sun.identity.agents.config.webservice.responseprocessor
com.sun.identity.agents.config.webservice.autherror.content
com.sun.identity.agents.config.webservice.enable
```

```
com.sun.identity.agents.config.webservice.endpoint
com.sun.identity.agents.config.jboss.webauth.available
com.sun.identity.agents.config.webservice.internalerror.content
com.sun.identity.agents.config.webservice.process.get.enable
com.sun.identity.agents.config.webservice.authenticator
com.iplanet.am.session.client.polling.enable
com.sun.identity.policy.client.resourceComparators
com.sun.identity.agents.config.policy.advice.use.redirect
```

+ *Properties Removed from Web Agents*

```
com.sun.identity.agents.config.cleanup.interval
com.sun.identity.client.notification.url
com.sun.identity.agents.config.debug.file.rotate
com.sun.identity.agents.config.remote.logfile
com.sun.identity.agents.config.local.log.rotate
com.sun.identity.agents.config.cdsso.enable
com.sun.identity.agents.config.cdsso.cdcservlet.url
com.sun.identity.agents.config.auth.connection.timeout
com.sun.identity.agents.config.poll.primary.server
com.sun.identity.agents.config.locale
com.sun.identity.agents.config.ignore.preferred.naming.url
com.sun.identity.agents.config.ignore.server.check
com.sun.identity.agents.config.convert.mbyte.enable
com.sun.identity.agents.config.proxy.override.host.port
com.sun.identity.agents.config.iis.auth.type
com.sun.identity.agents.config.iis.filter.priority
com.sun.identity.agents.config.iis.owa.enable
com.sun.identity.agents.config.iis.owa.enable.change.protocol
com.sun.identity.agents.config.iis.owa.enable.session.timeout.url
com.sun.identity.agents.config.domino.check.name.database
com.sun.identity.agents.config.domino.ltpa.enable
com.sun.identity.agents.config.domino.ltpa.cookie.name
com.sun.identity.agents.config.domino.ltpa.config.name
com.sun.identity.agents.config.domino.ltpa.org.name
com.sun.identity.agents.config.load.balancer.enable
com.sun.identity.agents.config.override.notification.url
```

- Several properties have been renamed:
  - The Realm property is now Policy Evaluation Realm.
  - The Application property is now Policy Set.
  - (Java Agents only) The Policy Client Polling Interval property is now Policy Cache TTL.
  - (Java Agents only) The PDP Cache TTL in Minutes property is now PDP Cache TTL in Milliseconds.
  - (Java Agents only) The Not-Enforced IP Invert List property is now Invert Not Enforced IPs.
  - (Java Agents only) The Alternative Agent Port Name property is now Alternative Agent Port Number.

- Improvements to the Documentation

  The AM documentation has been reorganized:

  - Some titles have been rewritten to better reflect the content.
  - Topics are split into individual pages within the book, to help organize content, and to help you locate the documentation you require when using search engines.
  - Reworked the Quick Start Guide into the Evaluation Guide. Use the new guide to quickly set up an AM deployment for evaluation purposes only.
  - Some topics are split into their own books now. For example, the information about sessions has been relocated from the Authentication and Single Sign-On Guide to the Session Guide.

    However, all security-related topics are now covered in the Security Guide. This guide will show you how to manage keystores and secrets, and how to secure realms, sessions, network connections, and others.

    The Setup and Maintenance Guide has also been split into two:

    - Follow the Setup Guide to perform tasks that you need to perform after installing AM, such as creating realms and adding external stores.
    - Read the Maintenance guide to learn about tasks and configurations you might repeat throughout the life cycle of a deployment in your organization. For example, monitoring and tuning instances.
  - Where possible, configuration reference is accessible from the relevant procedures. However, reference pertaining to global services is covered in the Reference.

- Configuration Upgrade Tool Distributed With AM ZIP

  The `AM-7.0.1.zip` file now includes a configuration file upgrade tool for converting configuration files exported with the **Amster** command. The tool is provided in the `Config-Upgrader-7.0.1.zip` file, which is inside the `AM-7.0.1.zip` file.

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*.

Chapter 2

Before You Install

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

Important Information Before Installing Access Management

Files to Download	Operating Systems	Web and Java Agents
Java	Application Containers	Directory Servers
Third-Party Software	Clients and Browsers	Special Requests

Important

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.

Files to Download

Access Management software is available at https://backstage.forgerock.com. "Access Management Software" describes the files available for download.

Access Management Software

File	Description
`AM-7.0.1.zip`	Cross-platform distribution including all software components. For a list of the files in the .zip archive, see "*Downloading AM*" in the *Installation Guide*.

File	Description
`AM-7.0.1.war`	Deployable web application archive file.
`AM-SSOAdminTools-5.1.3.8.zip`	The .zip file that contains tools to manage AM from the command line.
`AM-SSOConfiguratorTools-5.1.3.8.zip`	The .zip file that contains tools to configure AM from the command line.

Operating System Requirements

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

Supported Host Operating Systems

Operating System	Versions
Red Hat Enterprise Linux, Centos	7, 8
Amazon Linux	Amazon Linux 2018.03
SuSE	12, 15
Ubuntu	16.04 LTS 18.04 LTS
Windows Server	2016, 2019

Web and Java Agents Platform Requirements

The following table summarizes the minimum required version of web and Java agents:

Minimum Agent Version Required

Agent	Versions
Web Agents	5.0.1
Java Agents	5.0.1

AM supports several versions of web agents and Java agents. For supported container versions and other platform requirements related to agents, refer to the *Web Agents Release Notes* and the *Java Agents Release Notes*.

Java Requirements

The following table lists supported Java versions:

Supported Java Versions

Vendor	Versions
OpenJDK, including OpenJDK-based distributions: • AdoptOpenJDK/Eclipse Adoptium • Amazon Corretto • Azul Zulu • Red Hat OpenJDK ForgeRock tests most extensively with AdoptOpenJDK/Eclipse Adoptium.	11
Oracle Java	11

Web Application Container Requirements

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

Supported Web Application Containers

Container	Versions
Apache Tomcat	8.5, 9
IBM WebSphere Liberty	20.0.0.1
JBoss Enterprise Application Platform	7.2
Wildfly	12, 19

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 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.

Directory Server Requirements

This section lists supported directory servers.

As described in Generic LDAPv3 Configuration Properties in the *Setup 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

Directory Server	Versions	Configuration	Apps / Policies	CTS	Identities	UMA
Embedded Directory Services [a]	7.0	✔	✔	✔	✔	✔
External Directory Services/OpenDJ	4.0+	✔	✔	✔	✔	✔
File system-based	N/A	✔				
Oracle Unified Directory	11g R2				✔	
Oracle Directory Server Enterprise Edition	11g				✔	
Microsoft Active Directory	2016, 2019				✔	
IBM Tivoli Directory Server	6.4				✔	

[a]Demo and test environments only

Third-Party Software

ForgeRock provides support for using the following third-party software when logging ForgeRock Common Audit events:

Software	Version
Java Message Service (JMS)	2.0 API
MySQL JDBC Driver Connector/J	8 (at least 8.0.19)
Splunk	8.0 (at least 8.0.2)

Tip

Elasticsearch and Splunk have native or third-party tools to collect, transform, and route logs. Examples include Logstash and Fluentd.

ForgeRock recommends that you consider these alternatives. These tools have advanced, specialized features focused on getting log data into the target system. They decouple the solution from the ForgeRock Identity Platform systems and version, and provide inherent persistence and reliability. You can configure the tools to avoid losing audit messages if a ForgeRock Identity Platform service goes offline, or delivery issues occur.

These tools can work with ForgeRock Common Audit logging:

- Configure the server to log messages to standard output, and route from there.
- Configure the server to log to files, and use log collection and routing for the log files.

ForgeRock provides support for using the following third-party software when monitoring ForgeRock servers:

Software	Version
Grafana	5 (at least 5.0.2)
Graphite	1
Prometheus	2.0

For hardware security module (HSM) support, ForgeRock software requires a client library that conforms to the PKCS#11 standard v2.20 or later.

Supported Clients

Important

Support for Internet Explorer 11 ends August 17, 2021, in alignment with the announcement from Microsoft ending support for Internet Explorer 11.

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 14.04 LTS or later	✔	✔			✔		
iOS 9 or later	✔	✔					✔
Android 6 or later	✔	✔					

[a] *Native Apps* is a placeholder to indicate the platform is not limited to browser-based technologies. An example of a native app would be something written to use our REST APIs.

[b] Windows 10 only.

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 7.0.1 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 to Existing Functionality

This chapter covers both "Critical Changes" and "Important Changes" to existing functionality.

Critical Changes

As part of planning your upgrade, you need to consider that certain changes in later AM versions may have an impact on your environment. Usually, these changes are driven by changes in specification, security policies, or performance.

When possible, the upgrade process makes the appropriate changes on AM configuration. However, sometimes you will need to perform additional configuration based on your environment needs.

In addition to mandatory upgrade steps outlined in "*Upgrading AM Instances*" in the *Upgrade Guide*, if you are using features described in the following table you will need to perform additional upgrade tasks:

Critical Changes to Existing Functionality

AM Version	Component or Feature	Change
7	User Profile Whitelist	The profile attribute whitelist controls the information returned to non-administrative users when accessing `json/user` endpoints. Common profile attributes are whitelisted by default, but you need to add any custom attribute you want your non-administrative users to see. For more information, see "Configuring the User Profile Whitelist" in the *Upgrade Guide*.
	`/json/authenticate` Endpoint	When a client makes a call to the `/json/authenticate` endpoint appending a valid SSO token, AM returns the `tokenId` field **empty** if `HttpOnly` cookies are enabled. For example: `{ "tokenId":"", "successUrl":"/openam/console", "realm":"/" }`
	Secure Authentication Tree State Secret ID	An AES 256-bit key called `directenctest` must be available in the environment during upgrade, but it does not need to be the same key that AM provides on the default keystore.

AM Version	Component or Feature	Change
		After upgrade, ensure that the `am.authn.trees.transientstate.encryption` secret ID is always mapped to an existing, resolvable secret or key alias. Failure to do so may result in trees not working as expected.
	The Embedded DS	The embedded DS can only be used for single AM instances, for test and demo purposes. Sites are not supported. Sites using embedded DS servers must be migrated to external DS servers before upgrading.
	SAML v2.0 Secrets	AM 7 migrated SAML v2.0 to use secret stores. The upgrade process only creates the secret store files on the AM instance where you ran the upgrade process. For more information, see "Configuring Secret Stores After Upgrade" in the *Upgrade Guide*.
	`goto` and `gotoOnFail` Query Parameter Redirection	Redirection URLs for authentication services, agents, and SAML v.2.0 must be configured in the Validation Service in the *Authentication and Single Sign-On Guide* if they are not in the same scheme, FQDN, and port as AM, or are not relative to AM's URL.
	Web Agents of a Version Earlier than 5.6.3	Several properties that used to be configured as custom properties (`com.sun.identity.agents.config.freeformproperties`) have been added as regular properties. Due to this change, upgrading to AM 7 will overwrite the value of the original custom properties with the default value of the new UI properties. To work around this issue, perform one of the following actions: • Upgrade to Web Agents 5.6.3 or later before upgrading to AM 7. • After upgrading to AM 7, reconfigure the properties that you configured as custom properties in their new UI counterparts.
	Changes on the CTS Reaper Tuning Properties	AM 7 changes the way the CTS reaper searches for expired tokens. After upgrading, retune the CTS Reaper using the information in "Reaper Search Size" in the *Core Token Service Guide (CTS)*.
	OpenID Connect Clients Authenticating with JWTs	OpenID Connect clients authenticating with JWTs must include in the JWT a `jti` claim containing a unique identifier, in line with OpenID Connect Core 1.0 incorporating errata set 1.
	Cookie Filter	AM flags cookies as secure if they come through a connection marked as secure, or if they come through HTTPS. See "Managing the Secure Cookie Filter" in the *Security Guide*.
6.5.0.2 // 6.5.1	OAuth 2.0 Refresh Tokens	AM only issues refresh tokens to clients that have the `refresh token` grant type configured in their client profile.

AM Version	Component or Feature	Change
		After an upgrade to 6.5 or later using the UI or the **openam-upgrade-tool** .jar file, existing OAuth 2.0 clients are configured to use all grant flows, including the Refresh Token Grant flow. To configure the `refresh token` grant type manually, see "To Configure AM to Issue Refresh Tokens" in the *OAuth 2.0 Guide*.
6.5	Recovery Codes	Recovery Codes are encrypted, and existing codes are no longer displayed to the user. For more information, see "Upgrading Device Recovery Codes" in the *Upgrade Guide*.
	Secret Stores	AM 6.5 introduced secret stores for OAuth 2.0 and the persistent cookie module. The upgrade process only creates the secret store files on the AM instance where you ran the upgrade process. For more information, see "Configuring Secret Stores After Upgrade" in the *Upgrade Guide*.
	External Configuration Store	DS 6.5 introduced setup profiles, which pre-configure instances for different usages, such as CTS or configuration data. The default base DN for a DS configuration store instance (`ou=am-config`) is different than the default used by previous versions of AM (`dc=openam,dc=forgerock,dc=org`). You should not attempt to run multiple instances of AM where the configuration store base DNs do not match. Use the same configuration store base DNs when configuring external DS 6.5+ instances that will be used simultaneously alongside existing DS 6 or earlier configuration store instances. For more information, see "Preparing Configuration Stores" in the *Installation Guide*.
6	JSON Endpoints	AM's CSRF protection filter requires that either the `X-Requested-With` or the `Accept-API-Version` headers are included on requests to endpoints under the `json` root. For more information, see "Reviewing REST API Versions Before Upgrading" in the *Upgrade Guide*.

Important Changes

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

Important Changes in AM 7.0.1

- Ability to Configure a Failure URL in Server-Side Authentication Scripts

Server-side scripts can now redirect users to specific URLs after authentication failure. For more information, see "Redirecting the User After Authentication Failure" in the *Authentication and Single Sign-On Guide*.

Important Changes in AM 7

- Upgrading with Embedded DS Is Not Supported

  The embedded DS server is *not supported for production* in AM 7. Therefore, if you have a site configured with embedded DS, you must migrate it to an external DS store before upgrading to AM 7.

  See the KB article How do I migrate from an embedded to external DS/OpenDJ in AM/OpenAM (All versions)?.

  The embedded DS is deprecated in 7 and will be removed in a future release.

  As part of this change, the embedded DS does not support replication, and cannot be configured as part of a site. The relevant replication options for the installer UI and Amster have been removed.

  + *How Do I Know if my Deployment Uses the Embedded DS?*

    - (AM 6 or earlier) Go to Deployment > Servers > *Server Name* > Advanced, and check the value of the `com.sun.identity.sm.sms_object_class_name` advanced property.

      If the value is `com.sun.identity.sm.ldap.SMSEmbeddedLdapObject`, the server is an evaluation instance of AM, and is using an embedded DS instance as the configuration store.

    - In the server where AM is installed, check if the `opends` directory exists under the `/path/to/openam` directory.

      You may have migrated it to an external directory and not deleted the directory, though. Check the files in the `opends/logs` directory to determine if the embedded DS is running.

    - Go to Deployment > Servers > *Server Name* > Directory Configuration > Server, and check the value of the host name column.

      When using an external configuration store, the AM instances point to the FQDN of the load balancer in front of the DS cluster, or to the FQDN of the DS affinity deployment.

      When using an embedded configuration store, each AM instance points to its own hostname, since the embedded DS is stored alongside the AM instance.

- Directory Services 7 is Secure by Default and Requires Secure Connections

  Directory Services 7 introduces a *secure by default* approach. One aspect of this approach is that all connections to DS instances must be secure; for example, by using LDAPS.

To connect to a DS instance using LDAPS, AM requires access to the self-signed certificate that DS generates.

To provide these certificates to AM, you must use a *truststore* that contains the necessary certificates, and configure AM to use that truststore when starting up.

Note

Evaluation installs of AM attempt to automatically add DS's self-signed certificate to the truststore defined by the `javax.net.ssl.truststore` property.

If the property is not defined, it creates a copy of the JDK's default `lib/security/cacerts` truststore, names it `truststore`, and places it in `/path/to/openam/security/keystores/`.

For more information, see "Preparing a Truststore" in the *Installation Guide*.

- Changes to the `goto` and `gotoOnFail` Redirections

  Earlier versions of AM redirected the user to the URL specified in the `goto` and `gotoOnFail` query string parameters supplied to the authentication service, SAML v2.0 entities, or agents during login and logout. To harden security against phishing attacks, we recommended that you configure the Validation Service.

  By default, AM 7 only redirects to the URLs specified in those query string parameters if the URLs are in the same scheme, FQDN, and port as AM, or to URLs relative to AM. You *must* configure any other URL in the Validation Service.

  + *Do I Need to Add my URL to the Validation Service?*

    Consider an example AM deployment configured in `https://am.example.com:8443/am`:

URL	Needs to be configured in the Validation Service?
`http://am.example.com:8080/am/XUI/#login`	Yes, the scheme and port are different.
`https://am.example.com:443/am/XUI/#login`	Yes, the port is different.
`/am/XUI/#login`	No, the paths relative to the AM URL are trusted.
`https://mypage.example.com/app/logout.jsp`	Yes, the scheme, port, and FQDN are different.

  For more information, "Configuring Success and Failure Redirection URLs" in the *Authentication and Single Sign-On Guide*.

- Changes to Account Lockout in Authentication Trees

AM 7 introduces improvements when handling account lockout when using authentication trees.

The *Success* and *Failure* nodes now increment or reset the invalid attempts count, and check the user status property, when reached.

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

As part of these changes, the "Data Store Decision Node" in the *Authentication and Single Sign-On Guide* **does not** check the user status property. Tree evaluation continues along the True path if the credentials are correct and the user is found, even if the user status is set to inactive.

Tip

You can use the "Account lockout Node" in the *Authentication and Single Sign-On Guide* to check the user status property at any point in the authentication tree, provided that you have first obtained a username.

- The Default Password of the "Demo" Evaluation User Has Changed

  The password for the `demo` user, that AM creates for evaluation purposes, is changing in AM 7:

  Old password: `changeit`

  New password: `Ch4ng31t`

- SSO Token Not Returned When Authentication Endpoint Called with an Existing Session and `HttpOnly` Cookies Are Enabled

  When a client appends a valid SSO token to a call to the `json/authenticate` endpoint, earlier versions of AM return the SSO token again in the `tokenId`field of the JSON response, regardless of the flags configured for the session cookie. For example:

  ```
  {
      "tokenId":"AQIC5wM2...",
      "successUrl":"/openam/console",
      "realm":"/"
  }
  ```

  AM 7 now returns the `tokenId` field **empty** when `HttpOnly` cookies are enabled. For example:

  ```
  {
      "tokenId":"",
      "successUrl":"/openam/console",
      "realm":"/"
  }
  ```

  Remember that AM upgrades cookies to secure cookies (except the `amlbcookie` cookie) when requests arrive over a secure channel.

To check if `HttpOnly` session cookies are configured, see "Configuring HttpOnly Session Cookies" in the *Security Guide*.

Change any custom login pages or applications that were expecting the old response.

- AM Configuration Directory Structure Changed

  The location of numerous files and directories inside the AM configuration directory has moved, so that similar types of data are stored together.

  The following describes the new directories located within the AM configuration directory, for example /path/to/openam:

Directory	Description
`/path/to/openam/config`	Contains files used for configuring AM, for example, the `boot.json` file.
`/path/to/openam/security`	Contains directories for storing keys, keystores, and secrets.
`/path/to/openam/var`	Contains folders for transient, writeable data, such as audit and debug log files.

Note

New installations of AM 7 will have the new configuration folder layout described above. Upgrading from a previous version will leave the structure the same as in the previous version.

- Audit Event Whitelisting

  AM 7 introduces a whitelist that controls the information that can be logged in audit events. AM has a predefined whitelist built in that only records values that do not contain sensitive information.

  You can add additional allowed values to the whitelist that are recorded in audit events. You can also override the whitelist by adding items you do not want in the output to a blacklist. Anything added to the blacklist is not recorded in audit events.

  When upgrading from a previous version of AM, any blacklisted values are copied into the blacklist of the upgraded server, unless they do not exist in the builtin whitelist, and would therefore not be recorded anyway.

  For more information on audit logging, see "Implementing the Audit Logging Service" in the *Security Guide*.

- Admin UI and User UI

  In earlier versions of AM, all of the UI was located at `/openam/XUI`.

  In AM 7, the UI is now split in the following way:

  - User UI, which is located at `/openam/XUI`. This contains any end user pages. For example, login screens, and user profiles.
  - Admin UI, which is located at `/openam/ui-admin`. This contains any pages related to the administration of an AM server. Note, administrative logins are delegated to the User UI.

- Localizing User-Facing UI Text Requires Rebuilding the UI

  In earlier versions of AM, you could copy user-facing localization files in your custom AM `.war` file. Downloading, localizing, and rebuilding the UI was not necessary.

  AM 7 builds the localization text directly into the UI JavaScript files and, therefore, you need to rebuild the UI to apply the localization. Once rebuilt, redeploy the UI or pack it into your custom `.war` file.

  For more information about downloading and rebuilding the UI, see the UI Customization Guide.

- UI Templates and Partial Files Moved

  In AM 7, the location of the default UI templates and partials has moved, and are now located in the `/openam-ui-user/src/resources/themes/default/` directory.

  When customizing the layout of the user interface, AM uses the partials and templates from the `/themes/default` directory if an equivalent file is not found in your customized theme.

  As part of these changes, the following files have also moved:

Previous Location	New Location
`openam-ui/openam-ui-ria/src/resources/templates/admin/views/common/navigation/_TreeNavigationLeaf.html`	`openam-ui/openam-ui-user/src/resources/themes/default/partials/navigation/_TreeNavigationLeaf.html`
`openam-ui/openam-ui-ria/src/resources/templates/user/uma/views/resource/_DeleteLabelButton.html`	`openam-ui/openam-ui-user/src/resources/themes/default/partials/uma/_DeleteLabelButton.html`
`openam-ui/openam-ui-ria/src/resources/templates/user/uma/views/resource/_NestedList.html`	`openam-ui/openam-ui-user/src/resources/themes/default/partials/uma/_NestedList.html`
`openam-ui/openam-ui-ria/src/resources/templates/user/uma/views/resource/_UnshareAllResourcesButton.html`	`openam-ui/openam-ui-user/src/resources/themes/default/partials/uma/_UnshareAllResourcesButton.html`

  If you have customized any of the files above, ensure that you move them to the new location when upgrading to AM 7.

  For more information on customizing the user interface, see the UI Customization Guide.

- Debug Logging Now Uses Logback

  In earlier versions of AM, debug logging was configured by navigating to `Debug.jsp`.

AM 7 uses Logback for configuration of debug logging.

To configure debug logging in AM 7, either navigate to `Logback.jsp` to make temporary changes, or create a `logback.xml` configuration file in the AM classpath to make persistent changes to debug logging.

For more information on configuring Logback, see "*Debug Logging*" in the *Maintenance Guide*.

As Logback can be configured to provide the same functionality, the following properties that could be added to the `debugconfig.properties` file are no longer used in AM 7:

- `org.forgerock.openam.debug.prefix`
- `org.forgerock.openam.debug.suffix`
- `org.forgerock.openam.debug.rotation`
- `org.forgerock.openam.debug.rotation.maxsize`

The `Debug.jsp` page has also been removed.

- 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 7.0.1 and earlier), AM would store the servers as an orderedlist:

  ```
  $./ldapsearch -p 51636 -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:1636|01|02
     sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1636|01|02
     sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=xxx.example.com:1636|03|02
     sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=localhost:51636
     sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1636|03|02
  ```

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

  ```
  $./ldapsearch -p 51636 -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:1636|01|
  02,xxx.example.com:1636|03|02,localhost:51636,zzz.example.com:1636|01|02,zzz.example.com:1636|03|02
  ```

- `request_uri` Values Must Be Pre-Registered

  In earlier versions of AM, you could configure the OAuth 2.0/OpenID Connect provider to require clients to pre-register their `request_uri` values.

Now, pre-registration of `request_URI` values is mandatory, and the option to disable it has been removed.

- Advanced Server Property `opensso.protocol.handler.pkgs` Replaced

  In earlier versions of AM, you could configure the `opensso.protocol.handler.pkgs` property with a value of `com.sun.identity.protocol`.

  AM 7 replaces this property with the new `org.forgerock.openam.http.ssl.connection.manager` property, which must point to a class that implements the `org.forgerock.openam.http.SslConnectionManager` interface, which controls both keystore and truststore settings, as well as hostname verification.

  The property name and value will be corrected when upgrading from a previous version. However, if you have a value other than `com.sun.identity.protocol` then you must manually set the value of the new property, and create a new implementation of the `org.forgerock.openam.http.SslConnectionManager` interface.

- Changes to how Supported and Evolving APIs are Labelled in Javadoc

  AM 7 alters the way that an API is marked as "supported" or "evolving". To determine if something is supported or evolving, you may need to navigate up through the object hierarchy to see if a parent is labelled. Previously, each item was marked individually.

- `alg` Parameter Removed from Keys Returned by JWK URI Endpoints

  AM 7 removes the `alg` parameter from the keys returned by the JWK URI endpoints. As a result, each `kid` is now unique.

- Support for Encrypted ID Tokens Added to the OpenID Connect End Session Endpoint

  In earlier versions of AM, trying to end a session using an encrypted ID token resulted in failure since the request did not include enough information for AM to decrypt the token.

  To support ending sessions when ID tokens are encrypted, AM 7 requires that the request to the end session endpoint includes the client ID for which AM issued the ID token.

  This change diverges from the specification defined in the OpenID Connect Session Management 1.0-draft 5.

  For more information, see "/oauth2/connect/checkSession" in the *OpenID Connect 1.0 Guide*.

- SAML v2.0 Failover is Enabled by Default

  In earlier versions of AM, you had to manually enable SAML v2.0 failover, by navigating to Configure > Global Services > SAML v2.0 Service Configuration > Global Attributes, and then selecting the Enable SAML v2.0 failover option.

  In AM 7, the Enable SAML v2.0 failover option is enabled by default and cannot be changed. The option no longer appears in the user interface.

For more information, see "Session State Considerations" in the *SAML v2.0 Guide*.

- SAML v2.0 RelayState Redirection Restricted to Same Domain as the AM Instance

  AM 7 alters the behavior of the Relay State URL List whitelisting property. If you do not specify any URLs in this property, AM will only redirect to URLs that match its deployment domain; for example, `example.com`.

  To be able to redirect using the RelayState parameter to a URL that does not match the instance of AM, you **MUST** add the URL to the Relay State URL List property.

  For more information, see Relay State URL List - Hosted IDP in the *SAML v2.0 Guide* or Relay State URL List - Hosted SP in the *SAML v2.0 Guide*

- Supported and Evolving APIs May Require Recompilation

  The method signature or imports of some supported and evolving APIs may change between versions of AM. We recommend recompiling any customizations implementations you have for each new version of AM.

  For example, the following classes related to the Service Management Service (SMS) have changed. Custom implementations that use any of the following require recompiling:

  `com.sun.identity.sm.ChoiceValues`

  The class now extends a parent interface that adds no additional methods to implement.

  `org.forgerock.openam.secrets.Secrets`

  The import for this evolving API class has changed.

- The **ssoadm** Command Now Requires a User DN

  The value for the `-u` parameter when using the **ssoadm** command now requires the full DN of an administrative user.

  For example:

  ```
  $ ./ssoadm list-servers -u uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org -f $HOME/.pwd.txt
  ```

  For more information, see "To Set Up Administration Tools" in the *Installation Guide*.

- LDAP Connection Pool Property Name Corrected

  The `com.sun.am.ldap.connection.idle.seconds` property has been corrected. If you have any files or scripts which have the previous spelling, `com.sun.am.ldap.connnection.idle.seconds`, you should correct them to the new, correct spelling.

  For more information about this property, see "Tuning LDAP Connectivity" in the *Maintenance Guide*.

- Service Configuration Notifications Processed Sequentially by Default

  The `com.sun.identity.sm.notification.threadpool.size` property now defaults to `1`, which causes notifications to be processed sequentially, avoiding any potential out-of-order conditions.

  For more information about this property, see "Notification Settings" in the *Maintenance Guide*.

- Using the Device Profile Authentication Nodes Requires an Identity Repository Schema Update

  If you intend to use the ForgeRock SDKs with the new device profiling authentication nodes that are in AM 7, you may need to update the schema in your identity repository.

  You should update the schema if any of the following are true:

  - You are upgrading AM from a previous version and use an external identity repository.

    See "To Upgrade From a Supported Version" in the *Upgrade Guide*.

  - You are installing a new AM instance and use an external identity repository.

    See "To Install and Configure Directory Services for Identity Data" in the *Installation Guide*.

- Removed Default Value of the Json Web Key URI Field for OAuth 2.0/OpenID Connect Clients

  When creating a new OAuth 2.0 or OpenID Connect client, earlier versions of AM set the value of the Json Web Key URI field to the `jwk_uri` endpoint in AM. For example, `https://openam.example.com:8443/openam/oauth2/connect/jwk_uri`.

  The value of the Json Web Key URI field in the client should not be AM's `jwk_uri` endpoint, but an external URL holding the client's public JWK.

  New clients created in AM 7 will have this field empty to avoid confusion, but existing clients will not be modified after upgrade.

- Changes in AM CTS Reaper Tuning Properties

  AM 7 changes the name and behavior of some of the advanced server properties used to tune the AM CTS reaper searches:

  - The default value of the `for org.forgerock.services.cts.reaper.search.pollFrequencyMilliseconds` property has changed from `300000` to `5000` milliseconds (from 5 minutes, to 5 seconds).
  - The `org.forgerock.services.cts.reaper.search.pageSize` property has been replaced with the `org.forgerock.services.cts.reaper.search.tokenLimit`.

    In earlier versions of AM, if the amount of expired tokens was larger than the value of the `pageSize` property, the CTS reaper would make multiple requests of the value of the `pageSize` property until all expired tokens were deleted.

    On environments with very large amounts of expired tokens, this could lead to very long pruning cycles that could cause a performance degradation on the CTS token store.

In AM 7, the CTS reaper makes one request of the value of the `tokenLimit` property, then sleeps for the value of the `org.forgerock.services.cts.reaper.search.pollFrequencyMilliseconds` property.

Requesting the reaper to run more times and recover smaller amounts of tokens avoids the performance impact of the previous implementation.

We recommend that you retune the CTS reaper after upgrading the AM to account for these changes.

For more information and recommendations about these properties, see "Reaper Search Size" in the *Core Token Service Guide (CTS)*.

- JWT ID Parameter (jti) Required in OpenID Connect JWT Client Authentication

  AM 7 now requires that OpenID Connect clients authenticating with a JWT include a `jti` claim in the JWT containing a unique identifier, in line with OpenID Connect Core 1.0 incorporating errata set 1.

  If the claim is missing, AM returns an HTTP 400 `invalid_request` error with the `JWT ID is missing` message.

  For more related information, see "Authenticating Clients Using JWT Profiles" in the *OAuth 2.0 Guide*.

- Changes to the Audit Logging Service

  AM 6.5 introduced the `AM-IDENTITY-CHANGE` and `AM-GROUP-CHANGE` audit events to log user and group-related changes our updates such as password changes, user creation and deletion, and others.

  AM 7 does not log this information by default, since doing so may have a performance impact on the AM instances.

  To configure whether the Audit Logging Service should log these events, AM 7 includes the `org.forgerock.openam.audit.identity.activity.events.blacklist` advanced server property, which also enables and disables the logging of `AM-ACCESS-ATTEMPT` events.

  This property replaces the `org.forgerock.openam.audit.access.attempt.enabled` advanced server property, which has been removed.

  For more information, see "Advanced Properties" in the *Reference*.

- Changes to the User Self-Service Flows

  AM 7 no longer reports if an account does not exist while recovering a username or password, or if an account already exists when registering a new one:

  - Recovery Flows

When KBA or email are enabled as security methods, the flow will not stop when the user introduces the invalid username. Instead, AM does one of the following, depending on which security method is configured:

- Presents the user with a random KBA question before failing.
- Presents the user with a message similar to `An email has been sent to the address you entered. Click the link in that email to proceed`, but does not actually send an email.

If both methods are configured, then AM presents the user with the email message.

- Registration Flow

  When email is enabled as a security method, AM presents the user with a message similar to `An email has been sent to the address you entered. Click the link in that email to proceed`, and then sends an email with a registration link to the address that the user entered.

  Clicking on the link sends the user to the registration page again, and AM shows a message similar to `One or more user account values are invalid`.

- WDSSO: Absolute Path of Keytab File Must Be Specified

  When configuring the Windows Desktop SSO (WDSSO) authentication module, the absolute path of the keytab file must be specified, instead of the URL.

  + *See an Image of the WDSSO Keytab File Field*

Chapter 5
Deprecated Functionality

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

Deprecated in AM 7.0.1

- The SOAP STS service is deprecated and will be removed in a future release. Installing instances of this service in AM 7.0.1 is not supported. However, upgrading existing instances is.

Deprecated in AM 7

- Deprecated Embedded Directory Services

  The availability of the embedded DS instance is deprecated in AM 7.

  You can use it for evaluation and demonstration purposes only in AM 7.

  The embedded DS server will be removed in a future version of AM. You should switch to external DS servers.

  For more information, see "*Preparing External Stores*" in the *Installation Guide*.

- Deprecated Authentication Chains and Modules

  Authenticating by using authentication chains and modules is deprecated in AM 7, and they will be removed in a future version of AM.

  You should migrate your environments to *Intelligent Access* using authentication trees and nodes.

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

- Deprecated Unused Authentication Methods in Hosted IDP Authentication Context Mapping

  Support for the following authentication methods in the Authentication Context table when configuring a hosted identity provider has been deprecated in AM 7:

  - `User`
  - `Role`

- `Resource URL`

The other authentication methods are not deprecated, and can be used to achieve the same results as the deprecated options.

For more information about configuring SAML v2.0 authentication context mappings, see Authentication Context in the *SAML v2.0 Guide*.

Chapter 6
Removed Functionality

Functionality listed under this section has been removed from AM.

Removed in AM 7.0.1

- Installing instances of the SOAP STS service in AM 7.0.1 is not supported. However, upgrading existing instances is.

Removed in AM 7

- Removed /openam/cdservlet

  The `cdservlet` servlet, which was used by Web Agents and Java Agents earlier than version 5 to accomplish CDSSO, has been removed from AM 7.

  As a result, the following has also been removed:

  - The classic CDSSO mode.
  - The following AM advanced server properties:
    - `com.iplanet.services.cdc.invalidGotoStrings`
    - `org.forgerock.openam.cdc.validLoginURIs`
  - The `com.sun.identity.federation.services.idpLoginURL` JVM property.

  IDFF `cdservlet`-related legacy audit log events are no longer logged.

- Removed Support for SAML v1.x

  Support for SAML v1.x has been removed from AM 7. However, AM 7 does support SAML v2.0.

  For more information about SAML v2.0, see the SAML v2.0 Guide.

- Removed Supported APIs

  AM 7 removes the following APIs from the `com.sun.identity.authentication.AuthContext` class, to allow AM to support Java 11:

  - constructor: `public AuthContext(String orgName, String nickName)` throws AuthLoginException

- constructor: `public AuthContext(String orgName, String nickName, URL url)` throws AuthLoginException
- method: `public static void setCertDBPassword(String password)`.

The following APIs have also been removed:

- Deprecated `SAE_PARAM_APPID` field removed from the SecureAttrs class.
- Deprecated `SiteAttributeMapper` and `PartnerSiteAttributeMapper` interfaces removed.

  Instead, use the ConsumerSiteAttributeMapper interface.
- Deprecated `getAttributeMapForFedlet` method removed.

  Instead, use the getAttributesForFedlet method.

- Removed the SAML v2.0 Service Configurations Service

  This service has been removed by realm. The metadata and signing aliases have been removed from the global service configuration, since the providers now use secret stores.

- Removed the `org.forgerock.services.cts.reaper.search.pageSize` CTS Reaper Advanced Server Property
- Removed the Dashboard Wizards

  The wizards in the Dashboard of the administrative users have been removed. They were using the JATO implementation of the UI, which is not supported with Java 11.

- Removed the `org.forgerock.openam.audit.access.attempt.enabled` Advanced Server Property

  It has been replaced with the `org.forgerock.openam.audit.identity.activity.events.blacklist` advanced server property.

  For more information, see "Advanced Properties" in the *Reference*.

Chapter 7

Fixes, Limitations, and Known Issues

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

Key Fixes

Key Fixes in AM 7.0.1

- OPENAM-16935: Logout issue after logging into AM with 'Remember my username' selected with iOS 14.0.1
- OPENAM-16934: sm.getSchemaManager has a typo including a comma
- OPENAM-16907: Kerberos Node in 7.0 does not work
- OPENAM-16877: Error when creating AM "Self-service Trees" service in native admin ui
- OPENAM-16848: Choice Collector and WDSSO node combination does not work if whitelisting is enabled
- OPENAM-16847: AM email service failing with 'Start TLS' option
- OPENAM-16838: AuthenticationApproachChecker does not handle session upgrade modules
- OPENAM-16823: IDM Nodes does not send or propagate transactionId tracking when contacting IDM
- OPENAM-16802: Upgrade from OpenAM 7.0 to 7.1.0 SNAPSHOT causes NPE
- OPENAM-16794: Google KMS options missing after upgrade from 6.5
- OPENAM-16791: AMAccessAuditEventBuilder#forRequest can generate an entry with :-1 for the port
- OPENAM-16769: Enabling Auto-federation when User Profile is Dynamic on SP causes SP to hang during SAML flow
- OPENAM-16759: Amster on windows : AM does not restart properly after setup
- OPENAM-16758: Cannot install AM 7 on Windows

- OPENAM-16745: client_id in access token ignores what's been registered when idm cache is disabled
- OPENAM-16703: OAuth2 Access token obtained from refresh token is certificate-bound regardless of "Certificate-Bound Access Tokens" configuration (when client_secret_basic used for credentials)
- OPENAM-16702: Saving engine configuration in FBC mode makes that config non-readable
- OPENAM-16701: The authorize endpoint with a service parameter will cause the parameter to appear as a PAP claim in the agent's ID token
- OPENAM-16697: Case mismatch for realm (when using legacy realm identifier format) on well-known endpoint results in issuer with incorrect path format
- OPENAM-16686: Cannot create a User after upgrade from 6.5.2 to 7.0.1
- OPENAM-16684: OIDC Dynamic Registration client_description cannot take String type
- OPENAM-16669: IdentityGateway Agent entry missing attribute required to support org.forgerock.openam.agent.TokenRestrictionResolver#getAgentInfo
- OPENAM-16650: Authz Policy Subjects Policy.title is showing property name text
- OPENAM-16641: OAuth2 provider supported grant types attribute missing localization property on XUI
- OPENAM-16606: Missing "org.forgerock.openam.saml2.authenticatorlookup.skewAllowance" property in server defaults
- OPENAM-16594: ssoadm help should be updated to reflect changes in AME-18650 / OPENAM-16155
- OPENAM-16583: Crucial information is missing when encountering LDAP connections issue.
- OPENAM-16555: (audit) logging does not tell which policy allowed or denied a resource request
- OPENAM-16551: Scalar String in OAuth2 Access Token Modification Script result in Unable to Obtain Access Token
- OPENAM-16545: Upgrade to AM 7.0.0 can cause problems with properties being overriden for some web agents
- OPENAM-16485: 'Failed Login URL' is not picked up from the auth chain
- OPENAM-16483: XUI - Typo in SAML SP "Default Relay State Url" label
- OPENAM-16368: Settings of Mail and Scripting global service properties are overwritten at upgrade
- OPENAM-16367: OIDC request_uri response causes NPE while debug logging
- OPENAM-16354: Concurrency bug in OAuth2ProviderSettingsFactory

- OPENAM-16338: Failing REQUISITE module after SUFFICIENT Device Match doesn't fail chain properly
- OPENAM-16157: Session Property Whitelist Service allows case variant Property Names but DS is not case sensitive
- OPENAM-16152: After upgrade, new Identity page has duplicate 'new identity' field and email address does not save
- OPENAM-16006: Device Code Grant does not work with Implied Consent as Authorization is not approved even after consented
- OPENAM-15671: LoginContext is missing debug logging for troubleshooting
- OPENAM-15663: UserInfoClaims is not part of public API
- OPENAM-14682: Microsoft Social Auth fails when creating an Microsoft account (Legacy OAuth2)
- OPENAM-14527: Microsoft Social Auth does not work with latest MS endpoints (Legacy OAuth2)
- OPENAM-11706: Policies in a policy set are not visible in Internet Explorer IE

Key Fixes in AM 7

- OPENAM-16433: Audit Logging change of behaviour when capturing "principals" and "userid" data for each authentication entry.
- OPENAM-16425: AM does not handle malformed/incorrect signature correctly
- OPENAM-16402: The passwordpolicy.allowDiagnosticMessage should be applicable to admin and selfservice password change.
- OPENAM-16379: URL fragments like # cause forbidden login in the XUI
- OPENAM-16284: XUI does not handle Special Chars / UTF-8 in realms properly.
- OPENAM-16279: AgentsRepo cannot recover when it fails especially on external Application store.
- OPENAM-16251: OIDC authentication request with parameters 'prompt=none' and 'acr_values=' triggers authentication
- OPENAM-16240: REST STS under subrealm cannot generate id_token with realm claim
- OPENAM-16233: Policy evaluation fails when subject not found (even in ignore profile)
- OPENAM-16214: Push Authentication Module does not work on Session Upgrade when User Cache disabled
- OPENAM-16184: Zero Page Login Collector does not work with UTF-8 base 64 encoded usernames and passwords
- OPENAM-16165: social authmodule causes NullPointerException

- OPENAM-16164: social authmodule fails if OIDC provider uses algorithm RS256 to sign Id Token
- OPENAM-16136: queryFilter only matches against first entry in array
- OPENAM-16132: When TtlSupport is enabled, Stateless OAuth2 Refresh token and JWT whitelist fails on synchroniseExpiryDates
- OPENAM-16032: Unable to delete devices with Recovery Code Collector Decision Node
- OPENAM-16031: Intermittent error message when concurrent obtain SSO Token ID with session quota constraints
- OPENAM-16014: An invalid user passed to any WebAuthn node throws NPE and breaks the Tree flow
- OPENAM-16013: Mismatched kid from Json Web Key URI when Specified Encryption Algorithm
- OPENAM-16009: Windows Desktop SSO node full adoption and compliance with tree node specifications
- OPENAM-15989: OAuth2 client_id should be url-decoded when using basic auth
- OPENAM-15982: OIDC - JWT Request Parameter returns errors in query, not in the fragment when consent is denied
- OPENAM-15970: Access Token introspect Fails in subrealm after root realm modified
- OPENAM-15944: WS-Federation - RPSignin Request fails because config data is used unchecked
- OPENAM-15905: Login failure with Post Authentication Plugin on timed out Authentication session throws NullPointerException
- OPENAM-15900: Kerberos fails when used with IBM JDK
- OPENAM-15896: WS-Federation relying party initiated passive request - stuck at Account Realm selection
- OPENAM-15881: Custom AM User (amUser.xml) field does not use default values from the schema
- OPENAM-15858: Auth Tree fails before 'Max Authentication Time' is reached if authentication session state management scheme CTS is used
- OPENAM-15853: External UMA store fails on resource creation
- OPENAM-15805: idtokeninfo endpoint gives invalid signature error when ID Token is expired
- OPENAM-15785: OIDC spec violation - HTTP POST can not be used to send Authentication Request
- OPENAM-15784: Form elements in policy environment condition tab are displayed twice
- OPENAM-15766: LoginState - account lockout is checkout although AM AccountLockout is disabled
- OPENAM-15758: KeyStore Secret Store fails to start due to secretId having some characters.

- OPENAM-15750: ERROR: OAuth2Monitor: Unable to increment "oauth2.grant" metric for unknown grant type BACK_CHANNEL
- OPENAM-15724: SAML2 entities do not set amlbcookie if there is only one server
- OPENAM-15713: AM SP drop the 80 characters RelayState silently for HTTP Redirect
- OPENAM-15698: IdP-initiated SSO fails with error 'Error processing AuthnRequest. IDP Session is NULL'
- OPENAM-15697: Default ACR values from OAuth2 provider not taken into account
- OPENAM-15694: RestSTSServiceHttpRouteProvider causes memory leak by adding route for every access
- OPENAM-15679: The option "com.sun.am.ldap.connnection.idle.seconds" has a misspelling
- OPENAM-15670: DeviceIdSave auth module initialization fails if username is null
- OPENAM-15667: AM debug log does not tell which auth-module was handled - needed for troubleshooting
- OPENAM-15645: The &refresh=true|false parameter for _action=validate is not working as expected
- OPENAM-15632: OAuth2 Refresh token lifetime with -1 (never expires) cannot work with CTS TTL support
- OPENAM-15628: Grant-Set Storage Scheme for CTS does not work with CIBA Flow
- OPENAM-15627: Switching CTS Storage Scheme to "Grant-set" fails with stateless refresh-tokens created with "One-To-One"
- OPENAM-15579: AM cookies are not set after successful SP-initiated SSO flow if SP Adapter calls 'response.sendRedirect(String)'
- OPENAM-15559: OATH module broken in Japanese locale
- OPENAM-15533: WS-Federation doesn't work with Authentication Trees
- OPENAM-15530: OAuth2/OIDC - Resource Owner Password flow with a public client creates an AM session in CTS
- OPENAM-15520: XUI Localisation Falls Back To AM-Default "EN" Instead Of Language-Default
- OPENAM-15508: moduleMessageEnabledInPasswordGrant does not apply to Trees
- OPENAM-15507: 500 error when calling /revoke or /refresh endpoint with wrong token
- OPENAM-15501: Xml encryption 1.1 namespaces aren't always mapped to prefixes correctly
- OPENAM-15494: AM expects nonce request parameter in authorize request when no id_token will be returned

- OPENAM-15491: Self service password reset returns 500 Internal Server Error, when new password rejected by datastore password policies.
- OPENAM-15489: WebAuthN Auth Node Doesn't Respect UV=Discouraged During AuthN
- OPENAM-15465: Sending HTTP Callback from Inner Tree Evaluator Fails Authentication
- OPENAM-15459: When Encrypted Attributes on SP is set only with AutoFederation enabled, the attributes get decryption error
- OPENAM-15425: OIDC endsession - encrypted id_tokens are not supported
- OPENAM-15374: OpenID Client authentication with private_key_jwt and client_secret_jwt does not enforce required jti claims
- OPENAM-15355: PageNode with multiple InputNodes without value throws Unsupported InputOnlyPasswordCallback
- OPENAM-15349: Access Token request returns a 500 error
- OPENAM-15345: at_hash value generated does not take the latest modified access token
- OPENAM-15323: ROPC with tree throws "Internal Server Error (500)" when user credentials are incorrect using AuthTree
- OPENAM-15307: Trees Example is not working as expected OOTB to ?service=Example
- OPENAM-15303: Claims with multiple values in issued_token from REST STS represented inconsistently.
- OPENAM-15244: AM configuration does not perform schema extension for identity store although it has the permissions
- OPENAM-15210: Authentication nodes that is assigned AuthType values may not work in Session Upgrade case with custom modules
- OPENAM-15164: CDSSO with "ignore profile" throws "No OpenID Connect provider"
- OPENAM-15160: LDAP Decision Node throws NPE when custom ldap server returns LDAP code 50 on bind
- OPENAM-15150: Upgrade fails when there is a bad Token Signing ECDSA public/private key pair alias field
- OPENAM-15147: HTTP 500 upon accessing openam/json/
- OPENAM-15145: OpenAM Scope Validator calls getUserInfo twice when creating IdToken
- OPENAM-15121: Persistent Cookie Auth Tree does not work after the second relogin (with browser closed)
- OPENAM-15117: KeyVault KeyStoreType not supported

- OPENAM-15116: Auth ID jwt can be modified to determine whether a realm exists or not
- OPENAM-15105: Unable to get trusted devices using REST API
- OPENAM-15101: Remove the ability to disable XUI
- OPENAM-15089: SAML SLO - Allow RelayState to be a path-relative URL
- OPENAM-15076: webAuthn config does not allow for multiple origins under the same rpId
- OPENAM-15044: OpenID connect id_token bearer Module Unable to obtain SSO Token due to OpenIDResolver Caching
- OPENAM-15036: Cannot view/manage SAML IdP entity in console, imported from schema compliant meta data file
- OPENAM-15028: Cannot load metadata in ssoadm without extended metadata
- OPENAM-15012: OIDC - JWT Request Parameter returns errors in query, not in the fragment
- OPENAM-14995: IdP Initiated single logout only performs local logout if IdP session cannot be found in cache
- OPENAM-14991: Changes to boot.json are overwritten
- OPENAM-14979: NPE in UtilProxySAMLAuthenticatorLookup if there is a failure to find cached oldSession in sessionUpgrade
- OPENAM-14977: PKCE Code challenge method for Authorization Code if not set should use plain
- OPENAM-14966: Performing access_token with arbitrary text as trusted cert header causes server error
- OPENAM-14919: Unncessary 'Unable to parse packet received from RADIUS client' log entries in log file
- OPENAM-14901: XUI - SAML2 module doesn't redirect to IDP if it's 2nd in the chain
- OPENAM-14895: user identity creation fails with "Identity ***" of type user not found.
- OPENAM-14893: XUI displays multiple error messages when an authentication session times out
- OPENAM-14889: Upgrade of Peristent Cookie auth module fails
- OPENAM-14883: OAuth2/OIDC - Issuing client secret to Public clients during registration
- OPENAM-14881: AM Proxied authorization feature on DataStore does not work with locked or expired DJ accounts for password change (gives errorcode=123)
- OPENAM-14867: AuthType is not set for Authentication Tree (AnyKnownUserAuthzModule fails in AuthTree)

- OPENAM-14859: ROPC throws "Internal Server Error (500)" when 'Password Grant authentication service' is empty
- OPENAM-14858: When NameIDPolicy does not contain `Format=..`, remoteEntityID is passed as null
- OPENAM-14848: Insufficient debug logging in OpenID Connect authentication module
- OPENAM-14845: user info endpoint does not correctly handle Certificate Bound Access Tokens
- OPENAM-14829: AuthSchemeCondition doesn't return realm aware policy condition advice
- OPENAM-14825: OAuth2 Dynamic Registration with Software Statement triggers objectClass=* search
- OPENAM-14804: Memory leak when running UMA RPT soak test
- OPENAM-14799: Unable to update Agent profile using REST
- OPENAM-14794: User privileges are removed from group if another group is given same privilege
- OPENAM-14786: idpSingleLogoutPOST throws error 500 IllegalStateException on SLO
- OPENAM-14783: PKCS11 KeyStore does not work on IBM JVM
- OPENAM-14782: AuthTree created Session does not use per User Session Service settings
- OPENAM-14766: introspect and tokeninfo endpoints return Internal Server Error 500 in some invalid tokens
- OPENAM-14717: mailto attribute have space between ':' and mail address
- OPENAM-14694: Consent page still shows claim values even when supported claim description is omitted
- OPENAM-14651: OAuth2 GrantSet E-Tag Assertion Failures due to Stale Reads
- OPENAM-14581: handling ManageNameID fails if NameID does not include SPNameQualifier
- OPENAM-14578: WDSSO failing but no fallback...
- OPENAM-14573: amlbcookie is not secure when authenticating with trees
- OPENAM-14572: prompt=login destroys and creates new session
- OPENAM-14570: OAuth mTLS DN comparison fails when DER-encoding is different
- OPENAM-14548: consent page still shows what's been granted/removed as a result of OAuth2 scope policy evaluation
- OPENAM-14546: SSOADM access not audited to the ssoadm.access logs anymore
- OPENAM-14539: SAML SLO with multi protocols

- OPENAM-14529: UMA RPT expiry time incorrect in CTS
- OPENAM-14523: NullPointerException in IdP-initiated ManageNameIDRequest using SOAP Binding
- OPENAM-14503: SAML2 - Key Transport Algorithm - RSA OAEP must be supported
- OPENAM-14483: If there is no token, then landing on the AM login page will result in 2 getSessionInfo Requests = 401 UnAuthZ
- OPENAM-14480: AuthLoginException is lost
- OPENAM-14471: Failed to create root realm for data store (External Policy | Application)
- OPENAM-14465: SAML2 Artifact binding fails on multi-instance / multiserver IDP setup with SAML2 Failover on
- OPENAM-14464: XUI sends the following message "Loading custom partial "${partialPath}" failed. Falling back to default." to the browser console when a custom theme is used
- OPENAM-14450: userinfo typo in Claims.java
- OPENAM-14426: Unable to add external data store in AM (Policy | Application) when using TLS/SSL
- OPENAM-14419: Policy evaluation returns search results for all policies that match outside of specified application
- OPENAM-14393: CTS Operation Fails Entry Already Exists logged for SAML2 Authentication is done
- OPENAM-14391: Self Service Link not Display when Using Authentication Tree
- OPENAM-14378: 'Set Persistent Cookie' node sets domain cookies in only one domain despite multiple Cookie Domains set
- OPENAM-14369: Upgrading from OpenAM 13.5.0 with custom PAPs causes NPE failure
- OPENAM-14362: UMA load test fails with Invalid resource type error
- OPENAM-14353: Error Message not Displayed when Change Password does not Meet Password Policy
- OPENAM-14337: Fail gracefully when request OIDC token using "Pairwise" Subject Type and no Redirection URI is configured in client
- OPENAM-14313: Audit Logging - STS transformations create duplicate entries
- OPENAM-14310: CheckSession page indicates the session is not valid
- OPENAM-14294: am-external Git repository 6.5 have bad source

- OPENAM-14281: IdP Proxy relays wrong AuthnContextClassRef
- OPENAM-14239: FMSigProvider.verify NPE with null input for certificates
- OPENAM-14233: updated_at claim in the ID Token is returned as a string and not a number
- OPENAM-14232: Performance issue when creating resource_set in UMA with many existing resource_set
- OPENAM-14229: custom AuthorizeTemplate under theme not used
- OPENAM-14213: Cannot view SAML SP entity imported with missing AuthnRequestsSigned attribute
- OPENAM-14212: SAML redirect to login page fails if AM installed into the root context
- OPENAM-14200: Social auth modules do not work when AM is installed into the root context
- OPENAM-14189: effectiveRange of Time environment has issue
- OPENAM-14175: CTS updates on multivalue attributes may throws Duplicate values exception
- OPENAM-14174: AM shows Ldapter.delete exception when session expires is triggered
- OPENAM-14167: HTML tags are shown part of the messages in Change Password section of AD Authentication module.
- OPENAM-14147: arg=newsession in XUI just shows the "Loading..." page
- OPENAM-14115: Sample Auth module does not work in a chain when used with Shared-state
- OPENAM-14112: Using client-based sessions when acting as SP can lead to an out-of-date client-based session cookie
- OPENAM-14111: Refresh Token flow not enabled on OAuth2 Client can still use Refresh Token flow
- OPENAM-14062: Redirect to Failure URL does not occur when authentication tree is not interactive
- OPENAM-14054: XUI Custom templates and Partials not applied consistently
- OPENAM-14053: Cannot build openam-ui in Windows for Yarn using mvn
- OPENAM-14040: LdifUtils debug logging prints out wrong classname
- OPENAM-14018: Radius Authentication Module Primary and Secondary Radius Server help button shows server:port when it should be server
- OPENAM-13999: Custom node containing ConfirmationCallbacks fails when dropped in a page node.
- OPENAM-13991: 'issuer' value in .well-known/openid-configuration response is incorrect for a sub-realm

- OPENAM-13978: Session Upgrade - AuthLevel format changes
- OPENAM-13942: SAML2 Circle of Trust - REST Update doesn't update the metadata of the provider
- OPENAM-13934: saml2error.jsp fails with exception when malformed SAML2 response given
- OPENAM-13900: OAuth2 Device flow - duplicate user_code error after authenticating user
- OPENAM-13892: Erroneous "Response's InResponseTo attribute is not valid error "SAML2 failover is enabled" when it is not
- OPENAM-13890: Install.log logs AMLDAPUSERPASSWD for unprivileged demo user in plaintext
- OPENAM-13851: Rest STS cannot be created in the Console when upgrading to 6
- OPENAM-13831: RP-Initiated Logout does not handle state parameter
- OPENAM-13779: Session API - _action=refresh requires an admin token
- OPENAM-13764: Monitoring logs in ERROR for "Agent.configAgentsOnly:agent type = OAuth2Client"
- OPENAM-13720: Public API method LDAPUtils.convertToLDAPURLs can not handle IPv6 literals
- OPENAM-13490: Software Publisher Agent - Secret is not saved when creating an Agent
- OPENAM-13465: Dynamic client registration sets wrong subjectType
- OPENAM-13446: Social Auth Service doesn't redirect if already using another chain
- OPENAM-13419: LDAPPolicyFilterCondition doesn't set request timeout
- OPENAM-13324: /users/{user}/devices/trusted REST queryFilter expression does not work and acts as "true"
- OPENAM-13064: OAuth2 - SAML v.2.0 Bearer Assertion Grant - SubjectConfirmationData element should be optional
- OPENAM-13000: Custom authentication module with a single ChoiceCallback value is processed without confirmation
- OPENAM-12955: Resource Owner Password Credentials Grant does not work with trees
- OPENAM-12759: max_age should a number, not a string
- OPENAM-12574: SAML2Utils.sendRequestToOrigServer throws NullPointerException on processing Cookies
- OPENAM-12498: Authorization Grant response returns scope(s) in the URL
- OPENAM-12228: WebAgent REST API queryFilter expression does not work and acts all "true"
- OPENAM-12186: Introspect endpoint for RPT does not check the authorization scheme

- OPENAM-11921: Incorrect NameId Format offered for SAML2 auth module in console
- OPENAM-11863: CORSFilter position in web.xml should come before most filters
- OPENAM-11778: Getting accessToken using authorization_code result in Unhandled exception
- OPENAM-11338: OpenID Connect id_token bearer auth module mixes up aud, azp during verification
- OPENAM-10869: SAML2 Authentication module return "Unable to link local user to remote user" ambiguous.
- OPENAM-10843: When generating an OIDC token through STS a "kid" value is not specified
- OPENAM-10127: SessionMonitoringStore should only be instantiated when monitoring is enabled
- OPENAM-9931: Global Session Service - two fields with the exact same name (Redundant 'Global Attributes' setting should be removed)
- OPENAM-9777: Json Web Key URI in OAuth2 OpenID connect client config pre-populated incorrectly
- OPENAM-9459: 500 Internal Server Error from changePassword endpoint with AD repo
- OPENAM-5867: Data Store LDAP server (admin-ordered) list is reordered by OpenAM

Limitations

The following limitations and workarounds apply to this release:

- Evaluation Installation Limitations

  In some cases, installing AM for evaluation purposes will fail with a message similar to the following if the JDK's default truststore's permissions are `444`:

  ```
  $JAVA_HOME/lib/security/cacerts (Permission denied), refer to install.log under /usr/share/tomcat/
  access/var/install.log for more information.
  ```

  To work around this issue, locate the truststore that your container is using and change its permissions to `644` before installing AM:

  ```
  $ sudo chmod 644 $JAVA_HOME/lib/security/cacerts
  ```

  You can change the permissions back as they were originally after installing AM.

- Identity and Data Store Scaling Limitations

  The connection strings to the data or identity stores are static and not hot-swappable. This means that, if you expand or contract your DS affinity deployment, AM will not detect the change.

  To work around this, either:

- Manually add or remove the instances from the connection string and restart AM or the container where it runs.
- Configure a DS proxy in front of the DS instances to distribute data across multiple DS *shards*, and configure the proxy's URL in the connection string.

- SAML v2.0 UI Limitations

  The new UI supports SAML v2.0 IDP and SP entities only. After upgrade, entities that do not have IDP or SP roles will be listed, but cannot be inspected or edited using the UI. An error will display in the UI when trying to access these entities.

  Entities containing roles other than IDP and/or SP will only display the IDP and/or SP roles.

- Web Authentication (WebAuthn) Limitations

  AM 7.0.1 does not support the following functionality as described in the Web Authentication specification:

  Registration

  - Token Binding is not supported.
  - Web Authentication extensions are not supported.
  - Trust anchors are currently not supported.
  - Credential ID values are not verified against the credential IDs registered with all existing users.
  - The ECDAA signature of the Packed attestation format is not supported.

  Authentication

  - Token Binding is not supported.
  - Web Authentication extensions are not supported.
  - Signature counters are not supported.

  For more information about Web Authentication, see "*MFA: Web Authentication (WebAuthn)*" in the *Authentication and Single Sign-On Guide*.

- **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 `Realm Admin` privilege**

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

  - Delegated administrators with the `Realm Admin` 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 `Policy Admin` 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.

- Non-String JOSE Header Parameters in JWTs Are Not Supported

  AM ignores the content of non-string JWT header parameters, such as `jku` and `jwe`. Configure the public keys/certificates in AM instead, as explained in the relevant sections of the documentation.

- **Different AM Versions Within a Site Are Not Supported**

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

- **Use of Special Characters in Policy or Application Creation is Not Supported**

  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 from Different Vendors is Not Supported**

  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.

- **JCEKS Keystore Now Required 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 "Managing the AM Keystore" in the *Security 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.

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 7.0.1

- OPENAM-16939: IDM nodes does not follow proxy settings

Known Issues in AM 7

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-10427: LDAP connections created by the configurator wizard are never closed
- OPENAM-10554: AM installation fails if BASE_DIR is different from the path in .openamcfg
- OPENAM-10696: Login screen does not show mobile users feedback on failure
- OPENAM-11083: Delegated Admin cannot create Oauth2 Provider in realm
- OPENAM-11737: http.response.headers not populating in audit logs
- OPENAM-12207: Created OAuth2 client using curl request with defined scopes breaks the AM UI
- OPENAM-13513: Call Authentication Tree in a Radius Client
- OPENAM-13962: Errors during shutdown of AM
- OPENAM-14207: NullPointerException AM Console if IDPSSODescriptor is missing attribute 'WantAuthnRequestsSigned'
- OPENAM-14263: Bad title for External Data Stores secondary configuration page
- OPENAM-14290: Caching issue for 'users' REST endpoint
- OPENAM-14322: Servers -> Directory Configuration API Can Be Broken With Crafted Payload

- OPENAM-14343: AM console - localisation issue for algorithms in global Common Federation Configuration
- OPENAM-14404: Multiple calls being made to session endpoint by XUI when session cookie lost
- OPENAM-14494: In Firefox the text is cropped inside of the realm's card on Dashboard
- 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-14594: Possible thread-safety issue in OIDC pairwise subject identifiers
- OPENAM-14602: The API documentation for some Node API is missing methods/fields in 6.5/7
- OPENAM-14666: XUI - InternalError: "too much recursion" error can appear when Adding/Viewing/Updating realms
- OPENAM-14755: NullPointerException if auth module callback xml file can not be retrieved by ResourceLookup
- OPENAM-14834: JWT bearer grant implementation finds trusted JWT issuers by performing an unindexed search
- OPENAM-14837: Trusted Issuer lookup does not pick up modified issuer values
- OPENAM-14838: Trusted JWT issuer cache is refreshed inefficiently affecting other lookups
- OPENAM-14882: OAuth2 do not log scopes while using device code flow
- OPENAM-14887: TimerPool logs error during AM graceful shutdown
- OPENAM-14897: Default values for JWKs URI content cache timeout and miss timeout are not set on upgrade
- OPENAM-15027: React-select-multi component - when press enter on the 'x' of selected entry to delete it triggers the form submission instead
- OPENAM-15037: React-select-multi component - when press a key to add an entry the previously selected entry remains highlighted
- OPENAM-15253: Upgrade fails if external data store for Applications and Policies is used
- OPENAM-15351: During Upgrade Scripts are not updated
- OPENAM-15534: LDAP connection errors when using DS7 and rest2ldap test

- OPENAM-15609: CorsService API Descriptor text doesn't match functionality
- OPENAM-15699: _fields query parameter for API "Action" end point eg _action=refresh does not work as documented
- OPENAM-15727: JWT minted by oauth2/authorize does not have correct acr claim when an upgraded SSO token is used
- OPENAM-15791: The /json/groups endpoint is not accessible to the Agents
- OPENAM-15812: WebAuthN Node for a user with a webauthn profile for another site causes authenticator to complain using wrong security key
- OPENAM-15860: IdP Init SAML SSO results in two set-cookie: amlbcookie headers in SP Consumer response
- OPENAM-15861: NullPointerException in CollectionHelper.getServerMapAttrs
- OPENAM-15879: openam > ui-admin > entire sessions view disappears when querying with asterisk
- OPENAM-15892: ScriptingSchemaStep clears whitelist customisations on upgrade
- OPENAM-16068: Annotation based service implementation provides no way to deregister service listeners
- OPENAM-16076: An auth node config marked @password (type char[]) cannot also be Optional
- OPENAM-16105: AM Login UI cannot handle self service and SDK authentication callbacks
- OPENAM-16197: social authmodule does not send activaion email if un-authenticated SMTP server is used
- OPENAM-16202: Deleting SAML2 entities in console does not remove them from COT
- OPENAM-16229: Exceptions logged while upgrading to AM7
- OPENAM-16258: Resource login fails to work to Authenticate to Module instance
- OPENAM-16261: Node dev guide - CoreWrapper is not supported API
- OPENAM-16280: German login page translation is not complete
- OPENAM-16491: SAML Update introduces javascript calls that aren't available in IE8 and below (or IE11 using Enterprise mode)
- OPENAM-16515: Social auth - insufficient debug logging for troubleshooting
- OPENAM-16522: Device Save Node failed on Platform environment
- OPENAM-16539: userinfo endpoint does not return expected user attributes

- OPENAM-16545: Upgrade to AM 7.0.0 can cause problems with properties being overriden for some web agents
- OPENAM-16554: misplaced bufferingEnabled checkbox in New Syslog configuration
- OPENAM-16555: (audit) logging does not tell which policy allowed or denied a resource request
- OPENAM-16561: OAuth Consent screen does not apply theming
- OPENAM-16581: SAML No authentication context error with authn module init SSO

Chapter 8
Documentation Updates

The following table tracks changes to the documentation set:

Documentation Change Log

Date	Description
2021-03-24	The following changes were made to the documentation: • Updated "Supported Clients" to mention that support for Internet Explorer 11 ends August 17, 2021, in alignment with the announcement from Microsoft ending support for Internet Explorer 11. • Updated Improvements in AM 7 to mention that the `AM-7.0.1.zip` file includes a configuration file upgrade tool, in `Config-Upgrader-7.0.1.zip`, for converting configuration files exported with the **Amster** command. This file was listed in "*Downloading AM*" in the *Installation Guide*, but not mentioned in these *Release Notes*. • Updated "*Session Upgrade*" in the *Sessions Guide* to clarify that the `ForceAuth` parameter used with an authentication tree causes AM to issue a new session token, regardless of the security requirements.
2021-01-07	The following changes were made to the documentation: • Updated the "*Supported Upgrade Paths*" in the *Upgrade Guide* section to remove the upgrade path from OpenAM 13.X add the upgrade path from AM 7.x. • Updated the SameSite release note in AM 7 to add information about the new secure cookie filter. Also added a new section, "Managing the Secure Cookie Filter" in the *Security Guide*. • Removed information about Oracle Weblogic from the installation guide, since it is not supported in this version. • Added a new section, "OAuth 2.0 Scopes Policy Script API Functionality" in the *Authorization Guide*. • Updated the chapter "*The Scripting Environment*" in the *Getting Started with Scripting* to show how to obtain the Groovy and JavaScript engine version that AM is using. • Updated the What's New in AM 7 section and the SAML v2.0 guide. As part of hardening the security around the SAML v2.0 implementation that happened in

Date	Description
	AM 7, the URLs specified in the Assertion Consumer Service must exactly match the SP's scheme, FQDN, and port. • Added a new section, "Setting Session Properties" in the *Authentication and Single Sign-On Guide*.
2020-11-04	Initial Release of AM 7.0.1. The following changes were made to the documentation alongside this release: • Added an entry in Important Changes in AM 7 about changes to the Windows Desktop SSO (WDSSO) authentication module. • Added an entry in Important Changes in AM 7 about changes pertaining to User Self-Service. • Added the "Adding Audit Information" in the *Authentication and Single Sign-On Guide* section. • Added an entry in "Limitations" about JWTs containing non-string JOSE header parameters. • Improved the documentation about tuning LDAP connections in nodes and modules in "Tuning Authentication Node/Module LDAP Connections" in the *Maintenance Guide*. • Added information about how to determine if an existing session is present before using the "Get Session Data Node" in the *Authentication and Single Sign-On Guide*. • Added more information about how to configure the public key or HMAC secret in "Authenticating Clients Using JWT Profiles" in the *OAuth 2.0 Guide*. • Added more information about using the **ssoadm** command with secure connections in "*Setting Up Administration Tools*" in the *Installation Guide*. • Updated "Web or Java Agents SSO and SLO" in the *SAML v2.0 Guide* with Java Agent 5.7 and Web Agent 5.7 properties. • Updated JVM tuning properties in "Tuning JVM Settings" in the *Maintenance Guide* • Documented different commands to export policy and application store LDIF files in "Preparing Policy and Application Stores" in the *Setup Guide*. • Clarified the documentation about the OAuth 2.0 JWK URI cache settings in "To Create and Configure a Client Profile" in the *OAuth 2.0 Guide*. • Clarified the documentation about the SAML v2.0 hosted SP attribute map in "Hosted Service Provider Configuration Properties" in the *SAML v2.0 Guide*. • Corrected the "Device Tampering Verification" in the *Authentication and Single Sign-On Guide* documentation to say that the device determines the score, rather than the node or the ForgeRock SDKs.

Date	Description
	• Updated how to create an HTTPS connector for Tomcat in "Configuring AM's Container for HTTPS" in the *Installation Guide*. • Corrected the account mapper classes in "Example: Protecting a Web Site With OAuth 2.0" in the *OAuth 2.0 Guide*. • Added documentation about HTTP options when configuring a JVM proxy in front of AM in "*Preparing the Environment*" in the *Installation Guide*. • Added an entry in What's New in AM 7 for the Account Active Check authentication module, that was added in AM 7, but not documented at the time. • Added an entry in Important Changes in AM 7 about the `org.forgerock.openam.audit.identity.activity.events.blacklist` advanced server property. • Added an entry in "Limitations" about changing the permissions to the container's truststore to at least, `644` before installing AM for evaluation. • Updated the "Linking Identities Automatically with Auto-Federation" in the *SAML v2.0 Guide* section to use the new UI included in version 7. • Corrected the user required to perform policy evaluation with REST in "To Evaluate a Policy" in the *Authorization Guide*. • Corrected the procedure about SAML v2.0 chains and trees to only include chains, in "Linking Identities by Using Authentication Trees or Chains" in the *SAML v2.0 Guide*.
2020-08-30	Initial release of AM 7.

Appendix A. Release Levels and Stability Labels

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

ForgeRock Product Release Levels

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

Release Level Definitions

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

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

ForgeRock Product Stability Labels

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

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

ForgeRock Stability Label Definitions

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

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

Appendix B. Getting Support

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details on ForgeRock's support offering, including support plans and service level agreements (SLAs), visit https://www.forgerock.com/support.

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

  While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.