Oracle® Fusion Middleware

Oracle Access Management Bundle Patch Readme

OAM Bundle Patch 12.2.1.4.220113 Generic for all Server Platforms

F51339-01

January 2022

Oracle Access Management Bundle Patch Readme

This document describes OAM Bundle Patch 12.2.1.4.220113.

This document requires a base installation of Oracle Access Management 12c Patch Set 4 (12.2.1.4.0). This supersedes the documentation that accompanies Oracle Access Management 12c Patch Set 4 (12.2.1.4.0), it contains the following sections:

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.220113

Oracle Access Management 12.2.1.4.220113 BP includes the following new features and enhancements:

- **Support for OAuth Custom Claims Plugin**

For details, see the note `Oracle Access Manager (OAM) Federation Protocol OAUth - Elaborated Steps For <Patch:28228295> (Doc ID 2817030.1)` at https://support.oracle.com

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.210920

Oracle Access Management 12.2.1.4.210920 BP includes the following new features and enhancements:

- **OAM SAML 2.0 Supported Encryption Algorithms**

  OAM supports AES-GCM encryption modes.

  For details, see OAM SAML 2.0 Supported Encryption Algorithms and Changing Default Encryption Algorithm

- **Two-way SSL for OAP over REST Communication.**

  You can enable mutual authentication for OAP over REST between WebGate and OAM Server, therefore ensuring that the Server communicates with authentic clients.

  For details, see Enabling two-way SSL for OAP over REST

- **TOTP-based Multi Factor Authentication in OAM**

  You can configure MFA using the `configureMFA` command with `config-utility.jar`

  For details, see Configuring TOTP-based Multi Factor Authentication in OAM

- **Token Signing Using Third-Party Certificates**

  Access tokens can be signed using a self-signed key pair generated out-of-the-box. In this release, OAM extends the support to allow signing of access tokens using third-party key pairs.

  For details, see Token Signing Using Third-Party Certificates

- **Mutual-TLS (mTLS) Client Authentication in OAM**

  In TLS authentication, the server confirms its identity by producing a certificate (public key), which is then verified by the TLS verification process. In mTLS (mutual-TLS), along with the server, the client's identity is also verified. The TLS handshake is utilized to validate the client's possession of the private key corresponding to the public key in the certificate and to validate the corresponding certificate chain.

  For details, see Configuring Client Authentication and Configuring mTLS Client Authentication

- **Custom Claims**

  OAM extends the ability to define the custom claims using templates that can be configured at client or domain level. The custom claims can be included in all the access tokens, ID tokens and userinfo. You can also perform value transformation as well as value filtering of the custom claim.

For details, see Custom Claims

- **OAuth Access Token Maximum Size**

  Default OAuth access token length limit has been increased to `7500`. This value can be overridden using the OAuth Identity domain custom parameter: `accessTokenMaxLength`.

- **OAuth Client Update - Support for `PATCH` Request**

  Introduces support for `PATCH` request during modification of OAuth clients. With `PATCH` operation, OAM appends existing scopes with values from the request. Similar behavior is provided for redirect_uris, grant types, and custom attributes. The existing `PUT` operation replaces the contents of OAuth client parameters with the values from the request.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.210408

Oracle Access Management 12.2.1.4.210408 BP includes the following new features and enhancements:

- **Session Management Optimizations**

  Session Management Engine has been optimized and tuned to provide improved system performance under load.

  Also see, Database Tuning for Oracle Access Management in the *Tuning Performance Guide*

- **OAuth Refresh Token Management**

  OAuth Token Management capabilities have been enhanced with the ability to invalidate Refresh Tokens.

  For details, see Revoking OAuth Tokens in *Administering Oracle Access Management*

- **12c WebGates for Apache and IIS Web Servers**

  WebGates for IIS and Apache Web Servers are made available in this release.

  For details, see Installing and Configuring IIS 12c WebGate for OAM in *Installing WebGates for Oracle Access Manager*

- **Support for TLS 1.3 & FIPS 140-2**

  This release is compliant with the latest FIPS and TLS standards and versions.

  For details, see Enabling FIPS Mode on Oracle Access Management and TLS 1.3 and TLS 1.2 Support in Oracle Access Management in *Administering Oracle Access Management*

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.201201

Oracle Access Management 12.2.1.4.201201 BP includes the following new features and enhancements:

- **Proof Key for Code Exchange (PKCE) Support in OAM**

  Introduces PKCE support in the existing OAM OAuth Authorization Code Grant Flow. It can be used to enhance the security of the existing 3-legged OAuth, mitigating possible authorization code interception attacks. You can enable PKCE at the domain level or just for a specific client.

  For details, see Proof Key for Code Exchange (PKCE) Support in OAM in *Administering Oracle Access Management*

- **Keep the OAUTH_TOKEN Response Unset**

  OAM provides an option to not set the `OAUTH_TOKEN` cookie or header when SSO Session Linking is enabled. You must set the challenge parameter `IS_OAUTH_TOKEN_RESPONSE_SET` to `false`.

  > **Note:**
  >
  > If `IS_OAUTH_TOKEN_RESPONSE_SET` is not configured, or set to `true` then the `OAUTH_TOKEN` cookie/header is set.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200909

Oracle Access Management 12.2.1.4.200909 BP includes the following new features and enhancements:

- **Support for AWS Role Mapping Attribute in SAML Response**

  Introduces a new function that can be configured in SP Attribute Profile for supporting the AWS role mapping attribute in SAML response.

  For details, see AWS Role Mapping Attribute in SAML Response in *Administering Oracle Access Management*

- **Support for Attribute Value Mapping and Filters in OAM Federation**

  OAM federation supported Attribute Name Mapping. It extends the support for Attribute Value Mapping and Attribute Filtering features.

  For details, see Using Attribute Value Mapping and Filtering in *Administering Oracle Access Management*

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200629

Oracle Access Management 12.2.1.4.200629 BP includes the following new features and enhancements:

- **Support for SameSite=None Attribute in OAM Cookies**

  OAM adds `SameSite=None` attribute to all the cookies set by WebGate and OAM Server.

  > **Note:**
  >
  > – You must also download and upgrade to the latest WebGate Patch for this feature to work. For details, see the note `Support for SameSite Attribute in Webgate (Doc ID 2687940.1)` at https://support.oracle.com.
  >
  > – See also the note `Oracle Access Manager (OAM): Impact Of SameSite Attribute Semantics (Doc ID 2634852.1)` at https://support.oracle.com.

  Optional Configurations on OAM Server

  – If SSL/TLS is terminated on Load Balancer (LBR) and OAM server is not running in SSL/TLS mode, set the following system property in **setDomainEnv.sh**: `-Doam.samesite.flag.value=None;secure` Alternatively, you can propagate SSL/TLS context from the LBR or Web Tier to OAM Server. For details, see `Doc ID 1569732.1` at https://support.oracle.com.

  – To disable the inclusion of `SameSite=None` by OAM Server, set the following system property in **setDomainEnv.sh**: `-Doam.samesite.flag.enable=false`

  – To set `SameSite=None` for non-SSL/TLS HTTP connections, set the following system property in **setDomainEnv.sh**: `-Doam.samesite.flag.enableNoneWithoutSecure=true`

  Example - To add the system properties to setDomainEnv.sh:

  1. Stop all the Administration and Managed Servers.
  2. Edit the `$OAM_DOMAIN_HOME/bin/setDomainEnv.sh`, and add the properties as shown:

     ```
     EXTRA_JAVA_PROPERTIES="-Doam.samesite.flag.enable=false $
     {EXTRA_JAVA_PROPERTIES}"
     export EXTRA_JAVA_PROPERTIES
     ```

  3. Start the Administration and Managed Servers.

  Optional Configurations for WebGate

  – If SSL/TLS is terminated on LBR and OAM Webgate WebServer is not running in SSL/TLS mode, set the **ProxySSLHeaderVar** in the **User Defined Parameters** configuration to ensure that WebGate treats the requests as SSL/TLS. For details, see User-Defined WebGate Parameters.

- To disable inclusion of `SameSite=None` by OAM WebGate, set `SameSite=disabled` in the **User Defined Parameters** configuration on the console. This is a per-agent configuration.
- To set `SameSite=None` for non-SSL HTTP connections, set `EnableSameSiteNoneWithoutSecure=true` in the **User Defined Parameters** configuration on the console. This is a per-agent configuration.

> **Note:**
>
> In deployments using mixed SSL/TLS and non-SSL/TLS components: For non-SSL/TLS access, OAM Server and Webgate do not set `SameSite=None` on cookies. Some browsers (for example, Google Chrome) do not allow `SameSite=None` setting on non-secure (non-SSL/TLS access) cookies, and therefore, may not set cookies if a mismatch is found.
>
> Therefore, it is recommended that such mixed SSL/TLS and non-SSL/TLS deployments are moved to SSL/TLS Only deployments to strengthen the overall security.

- **X.509 Authentication with Extended Key Usage (EKU)**

  In X.509 authentication flows, Extended Key Usage (EKU) certification extension check can be added optionally to ensure that the usage of the certificate is allowed.

  For details, see X.509 Authentication Using Extended Key Usage (EKU) in *Administering Oracle Access Management* Management.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200327

Oracle Access Management 12.2.1.4.200327 BP includes the following new features and enhancements:

- **OAuth Consent Management**

  Provides capability for managing user consents, persisting user consents and providing mechanism to revoke them across DataCenters. Consent revocation capability is provided for both Administrators as well as individual users.

  For details, see Enabling Consent Management and Enabling Consent Management on MDC in *Administering Oracle Access Management*

- **OAuth Just-In-Time (JIT) User Linking and Creation**
  Provides capability to provision users automatically. The idToken as received from IDP has user attributes. These user attributes can have values like userId, user name, first name, last name, email address, and so on, which could be used for linking users to entries in the local id store or create them, if they do not exist.

  For details, see OAuth Just-In-Time (JIT) User Provisioning in *Administering Oracle Access Management*

- **OAM Snapshot Tool**
  Provides tooling to create a snapshot of the OAM IDM Domain with all its configurations, persist it, and use it for creating fully functional OAM IDM Domain clones.

  For details, see Using the OAM Snapshot Tool in *Administering Oracle Access Management*

- **SAML Holder-of-Key (HOK) Profile Support**
  SAML Holder-of-Key (HOK) profile support is added for OAM when acting as an Identity Provider (IP). This support is with OCI Service Provider (SP) Partners.

  For details, see the note `OAM 12c Identity Provider (IDP) for SAML Profile Support with OCI Service Provider (SP) Partners (Doc ID 2657717.1)` at https://support.oracle.com.

Understanding Bundle Patches

Describes Bundle Patches and explains differences between Stack Patch Bundle, Bundle Patches, interim patches, and patch sets.

- Stack Patch Bundle
- Bundle Patch
- Patch Set

Stack Patch Bundle

Stack patch Bundle deploys the IDM product and dependent FMW patches using a tool. For more information about these patches, see `Quarterly Stack Patch Bundles (Doc ID 2657920.1)` at https://support.oracle.com.

Bundle Patch

A bundle patch is an official Oracle patch for Oracle Fusion Middleware components on baseline platforms. In a bundle patch release string, the fifth digit indicated the bundle patch number. Effective November 2015, the version numbering format has changed. The new format replaces the numeric fifth digit of the bundle version with a release date in the form "YYMMDD" where:

- YY is the last 2 digits of the year
- MM is the numeric month (2 digits)
- DD is the numeric day of the month (2 digits)

Each bundle patch includes the libraries and files that have been rebuilt to implement one or more fixes. All of the fixes in the bundle patch have been tested and are certified to work with one another.

Each Bundle Patch is cumulative: the latest Bundle Patch includes all fixes in earlier Bundle Patches for the same release and platform. Fixes delivered in Bundle Patches are rolled into the next release.

Patch Set

A patch set is a mechanism for delivering fully tested and integrated product fixes that can be applied to installed components of the same release. Patch sets include all of the fixes available in previous Bundle Patches for the release. A patch set can also include new functionality.

Each patch set includes the libraries and files that have been rebuilt to implement bug fixes (and new functions, if any). However, a patch set might not be a complete software distribution and might not include packages for every component on every platform.

All of the fixes in the patch set have been tested and are certified to work with one another on the specified platforms.

Recommendations

Oracle has certified the dependent Middleware component patches for Identity Management products and recommends that Customers apply these certified patches.

For more information on these patches, see the note `Certification of Underlying or Shared Component Patches for Identity Management Products (Doc ID 2627261.1)` at https://support.oracle.com.

Bundle Patch Requirements

To remain in an Oracle-supported state, apply the Bundle Patch to all installed components for which packages are provided. Oracle recommends that you:

1. Apply the latest Bundle Patch to all installed components in the bundle.
2. Keep OAM Server components at the same (or higher) Bundle Patch level as installed WebGates of the same release.

Applying the Bundle Patch

The following topics helps you, as you prepare and install the Bundle Patch files (or as you remove a Bundle Patch should you need to revert to your original installation):

- Using the Oracle Patch Mechansim (Opatch)
- Applying the OAM Bundle Patch
- Applying the OAM Bundle Patch in Multi Data Center (MDC)
- Recovering From a Failed Bundle Patch Application

> **Note:**
>
> - Oracle recommends that you always install the latest Bundle Patch.
> - You must install libovd patch 20812896 and WLS patch 32698246.
>
> Bug 18957556 has a dependency on the libovd patch 20812896.

Using the Oracle Patch Mechanism (Opatch)

The Oracle patch mechanism (Opatch) is a Java-based utility that runs on all supported operating systems. Opatch requires installation of the Oracle Universal Installer.

> **Note:**
>
> Oracle recommends that you have the latest version of Opatch from My Oracle Support. Opatch requires access to a valid Oracle Universal Installer (OUI) Inventory to apply patches.

Patching process uses both unzip and Opatch executables. After sourcing the ORACLE_HOME environment, Oracle recommends that you confirm that both of these exist before patching. Opatch is accessible at: `$ORACLE_HOME/OPatch/opatch`

When Opatch starts, it validates the patch to ensure there are no conflicts with the software already installed in your $ORACLE_HOME:

- If you find conflicts with a patch already applied to the $ORACLE_HOME, stop the patch installation and contact Oracle Support Services.
- If you find conflicts with a subset patch already applied to the $ORACLE_HOME, continue Bundle Patch application. The subset patch is automatically rolled back before installation of the new patch begins. The latest Bundle Patch contains all fixes from the previous Bundle Patch in $ORACLE_HOME.

This Bundle Patch is not -auto flag enabled. Without the -auto flag, no servers needs to be running. The Machine Name & Listen Address can be blank on a default install.

> **See Also:**
>
> Oracle Universal Installer and Opatch User's Guide

Perform the steps in the following procedure to prepare your environment and download Opatch:

- Log in to My Oracle Support: https://support.oracle.com/

- Download the required Opatch version.
- Use `opatch -version` to check if your Opatch version is the latest. If it is an earlier version of Opatch, download the latest version.
- Confirm if the required executables opatch and unzip are available in your system by running the following commands:

  Run *`which opatch`* — to get path of opatch

  Run *`which unzip`*— to get path of unzip

  Check if the path of executables is in the environment variable "PATH" , if not add the paths to the system PATH.
- Verify the OUI Inventory using the following command:

  ```
  opatch lsinventory
  ```

  Windows 64-bit: `opatch lsinventory -jdk c:\jdk180`

  If an error occurs, contact Oracle Support to validate and verify the inventory setup before proceeding. If the `ORACLE_HOME` does not appear, it might be missing from the Central Inventory, or the Central Inventory itself could be missing or corrupted.
- Review information in the next topic Applying the OAM Bundle Patch

Applying the OAM Bundle Patch

Use information and steps here to apply the Bundle Patch from any platform using Oracle patch (Opatch). While individual command syntax might differ depending on your platform, the overall procedure is platform agnostic.

The files in each Bundle Patch are installed into the destination `$ORACLE_HOME`. This enables you to remove (roll back) the Bundle Patch even if you have deleted the original Bundle Patch files from the temporary directory you created.

> **Note:**
>
> Oracle recommends that you back up the $ORACLE_HOME using your preferred method before any patch operation. You can use any method (zip, cp -r, tar, and cpio) to compress the $ORACLE_HOME.

Formatting constraints in this document might force some sample text lines to wrap around. These line wraps should be ignored.

To apply the OAM Bundle Patch

Opatch is accessible at `$ORACLE_HOME/OPatch/opatch`. Before beginning the procedure to apply the Bundle Patch be sure to:

- Set `ORACLE_HOME`

For example:

```
export ORACLE_HOME=/opt/oracle/mwhome
```

- Run `export PATH=<<Path of Opatch directory>>:$PATH` to ensure that the Opatch executables appear in the system PATH. For example:

  ```
  export PATH=$Oracle_HOME/OPatch:$PATH
  ```

1. Download the OAM patch p33751903_122140_Generic.zip
2. Unzip the patch zip file into the PATCH_TOP.

   ```
   $ unzip -d PATCH_TOP p33751903_122140_Generic.zip
   ```

   > **Note:**
   >
   > On Windows, the unzip command has a limitation of 256 characters in the path name. If you encounter this, use an alternate ZIP utility such as 7-Zip to unzip the patch.

   For example: To unzip using 7-Zip, run the following command.

   ```
   "c:\Program Files\7-Zip\7z.exe" x p33751903_122140_Generic.zip
   ```

3. Set your current directory to the directory where the patch is located.

   ```
   $ cd PATCH_TOP/33751903
   ```

4. Log in as the same user who installed the base product and:
   - Stop the AdminServer and all OAM Servers to which you will apply this Bundle Patch.

     Any application that uses this OAM Server and any OAM-protected servers will not be accessible during this period.
   - Back up your `$ORACLE_HOME: MW_HOME`.
   - Move the backup directory to another location and record this so you can locate it later, if needed.
5. Run the appropriate Opatch command as an administrator to ensure the required permissions are granted to update the central inventory and apply the patch to your $ORACLE_HOME. For example:

   ```
   opatch apply
   ```
   Windows 64-bit: `opatch apply -jdk c:\path\to\jdk180`

   > **Note:**
   >
   > Opatch operates on one instance at a time. If you have multiple instances, you must repeat these steps for each instance.

6. Start all Servers (AdminServer and all OAM Servers).

Applying the OAM Bundle Patch in Multi Data Center (MDC)

Use information and steps here to apply the Bundle Patch in an MDC setup.

It is recommended that you upgrade or patch the Master data center followed by each of the Clone data centers.

Perform the following steps to apply the patch in an MDC setup.

1. Upgrade or apply the patch on the Master data center. For more information, see Applying the OAM Bundle Patch
2. Disable Automated Policy Synchronization (APS) between Master and the Clone data center that needs to be patched. For details, see Disabling Automated Policy Synchronization in *Administering Oracle Access Management*
3. Ensure that `WriteEnabledFlag` is `true` in oam-config.xml. If it is not enabled, set the `WriteEnabledFlag` to `true` in Clone data center using the following WLST commands.

```
connect('weblogic','XXXX','t3://localhost:7001')
     domainRuntime()
     setMultiDataCenterWrite(WriteEnabledFlag="true")
```

4. Upgrade or apply the patch on the Clone data center.
5. Change the `WriteEnabledFlag` to `false` in the Clone data center using the following WLST commands:

```
connect('weblogic','XXXX','t3://localhost:7001')
     domainRuntime()
     setMultiDataCenterWrite(WriteEnabledFlag="false")
```

> **Note:**
>
> Clone must be made write-protected before enabling APS to ensure that there are no inconsistencies between the data centers

6. Re-enable APS between Master and the upgraded Clone data center. For details, see Enabling Automated Policy Synchronization in *Administering Oracle Access Management*

Recovering From a Failed Bundle Patch Application

If the AdminServer does not start successfully, the Bundle Patch application has failed.

To recover from a failed Bundle Patch application

1. Confirm that there are no configuration issues with your patch application.
2. Confirm that you can start the AdminServer successfully.

3. Shut down the AdminServer and roll back the patch as described in Removing the Bundle Patch then perform patch application again.

Removing the Bundle Patch

If you want to rollback a Bundle Patch after it has been applied, perform the following steps. While individual command syntax might differ depending on your platform, the overall procedure is the same. After the Bundle Patch is removed, the system is restored to the state it was in immediately before patching.

> **Note:**
>
> - Removing a Bundle Patch overrides any manual configuration changes that were made after applying the Bundle Patch. These changes must be re-applied manually after removing the patch.
> - Use the latest version of Opatch for rollback. If older versions of the Opatch is used for rollback, the following fail message is displayed:
>
> ```
> C:\Users\<username>\Downloads\p33751903_122140_Generic\33751
> 903
> >c:\Oracle\oam12214\OPatch\opatch rollback -id 33751903
> Oracle Interim Patch Installer version 13.9.2.0.0
> Copyright (c) 2020, Oracle Corporation. All rights reserved.
> ......
> The following actions have failed:
> Malformed \uxxxx encoding.
> Malformed \uxxxx encoding.
> ```

Follow these instructions to remove the Bundle Patch on any system.

To remove a Bundle Patch on any system

1. Perform steps in Applying the OAM Bundle Patch to set environment variables, verify the inventory, and shut down any services running from the `ORACLE_HOME` or host machine.
2. Change to the directory where the patch was unzipped. For example:`cd PATCH_TOP/33751903`
3. Back up the `ORACLE_HOME` directory that includes the Bundle Patch and move the backup to another location so you can locate it later.
4. Run Opatch to roll back the patch. For example:

   ```
   opatch rollback -id 33751903
   ```

5. Start the servers (AdminServer and all OAM Servers) based on the mode you are using.
6. Re-apply the Bundle Patch, if needed, as described in Applying the Bundle Patch.

Resolved Issues

This chapter describes resolved issues in this Bundle Patch.

This Bundle Patch provides the fixes described in the below section:

Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Applying this bundle patch resolves the issues listed in the following table:

Table 1-1 Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Base Bug Number	Description of the Problem
33533200	AUTHZ CALL FAILS WHEN RDN HAS SPECIAL CHARACTER **Note:** This bug is dependent on libovd patch 33638694
33518405	Fix for Bug 33518405

Table 1-1 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Base Bug Number	Description of the Problem
33474333	MDC: FAILURE TO GET ACCESS TOKEN FROM AUTHZ CODE IN LOCAL DC **Note:** This is relevant only when different user identity stores are used for OAuth domain and Authentication Policy for OAuth consent resource. Following system property must be set in `setDomainEnv.sh` to enable this fix: `-Doam.sessionRetrievalWithId=true`
33368662	HTTPTOKENEXTRACTOR PLUGIN DOES NOT PUT HEADER NAME IN THE CREDENTIAL PARAMETER **Note:** Headers must be comma seperated, if more than one header is configured in `KEY_HEADER_PROPERTY` for `HTTPTOKENEXTRACTOR` plugin in the authentication module.
32923468	MDC: ADAPTIVE AUTHENTICATION MODULE
33389214	INVOKING THE OAM SESSION REST API GET BAD REQUEST ERROR.
33358965	CHANGE PASSWORD RULES APPEAR TO BE URL ENCODED ON THE /OTPFP/USERSELECT PAGE

Table 1-1 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Base Bug Number	Description of the Problem
33391677	FEDERATED USER HAVING \ IS SENDING \5C\ TO LIBOVD WITH FILTERESCAPE VALUE TRUE **Note:** This bug is dependent on libovd patch 33638694
33142450	USER STILL RETURNED TO THE URL EVEN WITH RETURNURLVALIDATIONENABLED
33069979	TAP INTEGRATION BETWEEN 12CPS4 OAM AND 11GR2PS3 OAAM IS NOT WORKING **Note:** You must enable the following system property to true: `oam.enable.legacy.client=true`. By default, it is false.
33242499	STRESS:FA:ATK:FMW12C: LOGON STORM TEST IS FAILING WITH 500 CLIENTS
33275487	STRESS:FA:ATK:FMW12C: CONCURRENTMODIFICATIONEXCEPTION SEEN IN OAM LOGS WHEN DIAGNOSTIC LOGGING ENABLED
33109073	OAMREAUTHENTICATE WORKS ONLY FIRST TIME

Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Applying this bundle patch resolves the issues listed in the following table:

Table 1-2 Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
33192650	"SYSTEM ERROR" ON THE CLONE DATA CENTER WITH OAM 12.2.1.4.210408 (BP06)

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
33214625	REDIRECT URI VALIDATION DOESN'T SUPPORT QUERY PARAMS, FRAGMENTS, ETC
33273701	CREATE CLIENT ARTIFACT ENDPOINT DOESN'T SUPPORT THE MEDIA TYPES MENTIONED IN REST DOCUMENTATION
33273732	NO GET API ON CLIENT/TRUST ARTIFACTS (ONLY POST OR DELETE AVAILABLE)
33273741	ISSUES WITH DISCOVERY END-POINT
33273750	TOKEN INTROSPECTION ENDPOINT DOESN'T CONFORM TO SPECIFICATIONS
32958613	JWT TOKEN CONTAINE GROUP IN INCORRECT FORMAT
33273674	MUTUAL TLS FOR OAUTH CLIENT AUTHENTICATION
33273579	CLI AND REST COMMANDS TO EASE SFA TOTP SETUP IN OAM
31517286	Fix for Bug 31517286
32102796	ALLOW SENDING ADDITIONAL CUSTOM CLAIMS INSIDE OIDC ID TOKEN WHEN OAM IS IDP
32201831	ABILITY TO PULL EMAIL VERIFIED CLAIM IN ID TOKEN FROM LDAP
30045443	OAM OAUTH: FEATURE TO GENERATE OAUTH TOKEN WITH TPC
33098826	UNSOLICITED LOGIN FLOW BREAKS WITH PASSWORD POLICY WITH SFA FLOW
33055065	FEDERATION NOT WORKING AFTER ACCESSING OAM PROTECTED PAGE
31431111	ON THE LOGOUT CONSENT PAGE, WORDING SHOW "SIGN IN" INSTEAD OF "SIGN OUT"
32761540	STRESS:FA:ATK:FTS ON AM_AUDIT_RECORD FROM SQL 8RWNP1YMTMWWB
33117541	NON-PROXY HOST EXCEPTIONS DO NOT WORK
33139217	OAM_ADMIN FAILS TO START AFTER APPLYING 12.2.1.4 APRIL/JULY 2021 BP
32920684	IMPORTPOLICYDELTA FAILS TO IMPORT ADVANCED AUTHENTICATION RULES
33084122	12C 21.07 EVNI: "ACCESS SERVER HAS RETURNED A FATAL ERROR WITH NO DETAILED INFORMATION" ERRORS IN OHS LOGS (WEBGATE)
33074398	ISSUE WITH APNS PATCH 32625905: SOUND MISSING
33010382	SPECIAL CHAR ON PASSWORD FIXED IN 29771448 & 31555915 NO LONGER WORK AFTER BP06
32807465	DELETING IDENTITY PROVIDER CANNOT REPLICATE TO CLONE SERVER FROM MASTER

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32704611	NOT ABLE TO CREATE OAUTH CLIENT IF ATTRIBUTE VALUE CONTAINS BACKSLASH **Note:** To enable backslash (\) attribute value, edit `setDomainEnv.sh` and add the following system property: `oracle.oam.oauth.allow.backslash`. The default value is `true`.
32909931	OAM NOT SETTING AUTHN RESPONSE HEADERS AFTER APPLY 12.2.1.4.210408
32543656	OAM 11G (SP) SHOULD END THE LOCAL SESSION WHEN RECEIVING SOAP LOGOUT REQUEST
32482754	INCREASE OAUTH ACCESS TOKEN MAXIMUM SIZE TO MORE THAN 5000 CHARACTERS
32879893	INTERMITTENT ERRORS IN OAM CONSOLE PREVENT VIEWING & UPDATING POLICY OBJECTS
32976735	EBS APPSLOGIN FAILS WHEN USING OAM WITH OUD AS BACKEND LDAP ON AIX WITH TLS 1.2 ONLY
32568653	12 VERSION : ACCESSSERVERCONFIGPROXY PORT CHANGING 5576 TO 5575 RESTARTADMIN **Note:** To trigger topology update, set the following system property in `setDomainEnv.sh` : `oam.t2p.enableTopologyUpdate=true`

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32953208	OAM OPENID CONNECT LOGOUT DOES NOT FORWARD STATE PARAMETER TO POST_LOGOUT_REDIRE
32933119	API /OAUTH2/REST/SECURITY DO NOT WORKING ERROR 406
27582324	POST DATA RESTORATION FAILS WHEN OBRAR.CGI USES GET METHOD TO RETRIEVE DATA.
31843528	ASSERTION HAS AN ADVICE ELEMENT THAT CONTAINS AN ENCRYPTED FIELD THAT FAILS OAM
32828842	OIDC-PIREAN INTEGRATION - NOT A VALID JWT TOKEN
32826737	TEST CONNECTION FOR LDAP IN OAM CONSOLE FAILS FOR TLS 1.2 ON IBM AIX **Note:** In IBM AIX OS 7.1 or 7.2 having OAM and OID set on TLSv1.2, ensure that you set the following OAM system property in `setDomainEnv.sh` : - `Djdk.tls.client.protocols=TLSv1.2` and restart the OAM Admin Server.
32734517	NOT ABLE TO UPDATE THE AUTHNSCHEMELEVEL FROM 5 TO 2 FOR X509 USING CURL
31859438	12C :OAUTH CLIENT : UPDATE : REDIRECT URI : SUPPORT FOR HTTP PATCH REQUEST

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32655233	LIBOVD 12C SPECIAL CHARACTER IN USERNAME FAILS TO LOCATE USER IN LDAP **Note:** This bug is dependent on libovd patch 32305678
32701831	REDIRECT LOOP USING INITIAL_COMMAND=NONE AFTER APPLICATION DOMAIN IDLE TIMEOUT
32501273	REMOTE IP NOT APPEAR INTO AUDIT DATABASE FOR OAUTH AUTHORIZATION
32653281	"FAILED TO INIT CONTEXT PATH:/IDAAS/AM/ESSO" ERROR IN ADMIN SERVER STARTUP LOGS

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32561825	AUTHMON - OAM AUTHMON (OAM-MON.SH) - NEED TO IMPLEMENT LOGOUT SO SESSIONS DO NOT BUILD UP.

Note:

In 12c PS4, OAM tester does not work in offline mode and is not supported through UI.
For command line support, update the OAM tester input xml, for example:

```
<case
uuid="a46c291
4-30c7-4b20-8
862-
c244fd0d74d5"
>
    <request
code="logout"
/>

<response
code="yes"
elapsed="178"
>

<comment></
comment>

<status>Major
 code:
2(NoCode)
Minor code:
2(NoCode)</
status>

<content></
content>
        </
```

Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
	response> </case>
32650194	FIX FOR BUG 32487114 IS NOT WORKING IN OAM REL13 PATCH 32628242
27584970	CAPACITY CONSTRAINT IN WEBLOGIC-APPLICATION.XML CAUSING PERFORMANCE IMPACT

Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

Applying this bundle patch resolves the issues listed in the following table:

Table 1-3 Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

Base Bug Number	Description of the Problem
32682922	SUCCESSFUL FEDERATION REDIRECTS TO RETURNURL EVEN THOUGH IT IS NOT WHITELISTED
31560646	FEDSTS ERRORS IN OAM LOGS

32680956	OAM OAUTH 12C NEED OUTPUT IN JSON FORMAT WHEN USING REST API
	`Accept` header is introduced in OAM OAuth REST APIs. If the `Accept` header is used, OAM returns the response in JSON format.
	For example:
	`curl --location --request GET \`
	`'http://<host>:<port>/oam/services/`
	`rest/ssa/api/v1/oauthpolicyadmin/client?`
	`identityDomainName=<DomainName>&name=<cli`
	`entName>' \`
	`--header 'Authorization: Basic`
	`d2VibG9naWM6V2VsY29tZTE=' \`
	`--header 'Accept: application/json' \`

Table 1-3 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

Base Bug Number	Description of the Problem

32625905	SUPPORT FOR HTTP/2 APPLE PUSH NOTIFICATION SERVER (APNS)
	Apple Push Notification Server (APNS) does not support legacy binary protocol from March 31, 2021. The new server (`api.push.apple.com:443`) supports only HTTP/2 protocol.
	This bug fix provides support for HTTP/2 protocol when using APNS. This feature is not enabled by default.
	To use HTTP/2 APNS perform the following steps:
	1. Ensure that Java 8 version is greater than 1.8.0_251.
	2. Set the `SfaUseAPNsHTTP2` property to `true` by running the `updateConfigProperty` WLST command. For example:
	`connect('ADMIN_USER','ADMIN_PASSWORD', 'ADMIN_HOST:ADMIN_PORT')`
	`domainRuntime()`
	`updateConfigProperty(propertyIdentifier="SfaUseAPNsHTTP2", propertyValue="true")`
	3. Restart the OAM server

32519715	USER FROM EXISTING SESSION IS DIFFERENT FROM USER LOCALLY AUTHENTICATED
32743560	OAM 12CP4 : FIX 32632139 IS FAILING OVER OAMSERVERCOMMUNICATIONMODE = HTTP
31629661	ASDK FAILS TO CONNECT TO RUNNING OAM SERVER.
32407903	"EXCEPTION IN DECRYPTION" ERROR DURING UNSOLICITED LOGIN AND LOGOUT VIA DCC WG
32376345	NEED ALTERNATE SOLUTION FOR 31186283 TO REDUCE EXTRA CALL TO OAM ENDPOINT
32198119	INVALID SESSION CONTROL PARAMETERS ERROR WHEN UPDATING GITO COOKIE DOMAIN
32291876	WEBGATE PROFILE GET CORRUPTED IF ADD PRIMARY/SECONDARY SERVER WITH INDEX = 2 USING WEBGATE TEMPLATE.
30116357	DCC WEBGATE WITH UNSOLICITED POST AUTHN FAILS AFTER APPLYING 02/19 PATCH

Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

Applying this bundle patch resolves the issues listed in the following table:

Table 1-4 Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

Base Bug Number	Description of the Problem
29244150	SSO BETWEEN TUNNELED DCC AND PLAIN DCC IS BROKEN WHEN APPLIED OAM BP'S 14,15 OR 16
27441865	CLIENTSSLKEYSTOREPWD, CLIENTSSLTRUSTSTOREPWD NOT PROPERLY WRITTEN IN OAM-CONFIG
28728420	OAM-OIM FIRSTLOGIN PAGE IS BLANK, BACKURL CONTAIN HOST IDENTIFIER
32612533	OAM 12CPS4 SSO BETWEEN FED SP1 AND SP2 PARTNER PROTECTED RESOURCE IS FAILING WITH APRIL BP 32525944
32153972	SIGNATURE VALIDATION FAILED OPENIDCONNECTPLUGIN CONFIGURATION
32392692	ORACLE CLOUD MCS_LOGIN_324.PNG NOT BEING USED AND APPEARS IN LOGIN PAGES
32632139	OAM 12CPS3 FIX FOR BUG 32055280 IS FAILING
32433361	ASDK INITIALIZATION FAILING
32477536	ASDK FAILED TO INITIALIZE IF COMPATIBILITYMODE IS OAM_12C
18957556	NOT GETTING P_ERROR_CODE=OAM-3 IN DIAGNOSTIC LOGS WHEN OID IS DOWN
29725629	Fix for Bug 29725629
31386392	NOTSTRESS:FA:ATK:ORACLE.OAM.BINDING ERRORS IN IDM WLS_OAM1 LOGS
27962394	USER WAS APPENDED WITH POD NAME
31994408	OAM LOGIN PAGES CHANGES TO ADAPT TO REDWOOD UI STYLE
30155115	OIFAUTOMATION.PL ENABLEOIF FAILURE - WRONG DB SCHEMA PASSWORD USAGE
31430985	IN THE INITIAL SIGN ON PAGE, THE TEXTBOX "USER ID" AND "PASSWORD" FIELD DOES NOT HAVE A LABEL
32430636	12C: 500 INTERNAL SERVER ERROR IN FAHOME PAGE
32394988	FOREGROUND AND BACKGROUND COLOURS DOES'T MEETS WCAG 2 AA CONTRAST RATIO THRESHOLDS
32487114	WCAG 2.0-2.4.1: PAGE MUST HAVE MEANS TO BYPASS REPEATED BLOCKS.
32451171	KM AUTOMATION : ADD AUTOMATION SCRIPT FOR CONFIG CHANGES IN BUG# 32380923
27481308	ER: OAM OAUTH PKCE (RFC 7636) SUPPORT

Table 1-4 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

Base Bug Number	Description of the Problem
32507312	ISSUE ACCESSING /OAMFED/USER/SLOOAM11G?ID=OAM11G&TYPE=3
29337161	12C UPDATES THE AM_SESSION TABLE IN THE DB FOR EVERY AUTHZ REQUEST
29951446	OAUTH SERVICE : TERMINATE TOKENS API NOT AVAILABLE
32380255	IOS PUSH NOTIFICATIONS PORTS 2195 AND 2196 ARE DEPRECATED FROM MARCH
32250953	INTERMITTENT LOGIN ISSUE WITH INTERNAL OAM ADC ENVIRONMENT
32428227	OAM_ADMIN DEPLOYMENT HAS FAILED
32134602	CONTINUATION OF BUG 31402491, USER FROM EXISTING SESSION IS DIFFERENT FROM USER
32340416	OAUTH REST API DELETE IDENTITY DOMAIN RETURNS SUCCESS WHEN INVALID REQUEST SENT
32245443	NULL POINTER EXCEPTION IS THROWN WHILE STARTING ADMINSERVER IF IAM SUITE APP DOMAIN IS MISSING.
30352121	NEED POSSIBILITY TO FILTER USER GROUPS SENT IN SAML RESPONSE IN FEDERATED ENV.
31776266	TOKEN HAS ACCESS TO CUSTOM ATTRIBUTES FOR ALL SCOPES
32167212	RESET OAM KEYSTORE PASSWORD IN 12C
31558236	SECURE FLAG IS NOT SET FOR SSL TERMINATED LOAD BALANCER
32051924	AFTER BP08 OLD CLIENTS STILL HAVE PLAIN TEXT SECRET
31900502	OAM12C - FORGOT PASSWORD WITH ONE-TIME PASSWORD DOESN'T WORK WITH SERVERREQUESTCACHETYPE FORM
31861713	OAM 12.2.1.4 IS NOT SENDING CLIENT CERTIFICATE DURING OUTBOUND ARTIFACT SAML REQ
31750371	SYSYEM ERROR AFTER REACHING INVALID OTP MAXATTEMPTS IN STANDALONE ENV
29971944	CONSENT PAGE FUNCTION FROM OIF 11GR1 NOT FOUND IN OAM 12C FEDERATION
32136382	NULLPOINTEREXCEPTION AFTER ADDING "-DORACLE.OAM.ENABLEEXTRASAMLATTR=TRUE"
31830597	OAUTH : ACCESS AND REFRESH TOKEN EXPIRY TIME NOT SET CORRECTLY
31822228	MFA FAILS WHEN ANONYMOUS SESSION EXISTS
30922965	UNABLE TO CREATE AND PERSIST USER..CAUSED BY: INVALID UUID STRING: ANONYMOUS-S

Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Applying this bundle patch resolves the issues listed in the following table:

Table 1-5 Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Base Bug Number	Description of the Problem
31266182	ACCESS TOKEN REQUEST WITH JWT BEARER GRANT FAILS WITH DB UNIQUE CONSTRAINT VIOLATION **Note:** For OAuth flows with MDC enabled, the parameter `SessionMustBeAnchoredToDataCenterServicingUser` must be set to `false` in the OAM Configuration.
30674083	OAUTH 3-LEGGED AUTHZ CODE CAN BE USED MORE THAN 1 TIME
28946202	OAM AUDITING NOT CAPTURING IAU_INITIATOR FOR FAILED AUTHENTICATION ATTEMPTS
31766587	OAM 12C-OPEN ID CONNECT-NONCE CLAIM MISSING IN TOKEN
31832371	REQUESTING OPTION TO LEAVE OAUTH_TOKEN RESPONSE UNSET WITH ER 29541818
31778001	Fix for Bug 31778001
30503494	AFTER AUTHENTICATION FAILURE USER DOES NOT REDIRECT TO FAILURE URL
31469921	MULTI VALUE ATTRIBUTES ARE NOT RETURNING VALUE FROM FEDERATION AT 12C
31734489	ERROR MESSAGE WHEN USER HAS EXCEEDED THE MAXIMUM NUMBER OF ALLOWED SESSIONS

Table 1-5 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Base Bug Number	Description of the Problem
31098504	FEATURE TO CONFIGURE THE ANONYMOUS USER ACCOUNT NAME You can configure username in the anonymous user session by modifying the `anonymousUserName` in the `oam-config.xml` file under `AnonymousModules`. For example: `<Setting Name="AuthenticationModules" Type="htf:map"> <Setting Name="AnonymousModules" Type="htf:map"> <Setting Name="89AS152C" Type="htf:map"> <Setting Name="validateUser" Type="xsd:boolean">false</Setting> <Setting Name="anonymousUserName" Type="xsd:string">GuestUser</Setting> <Setting Name="name" Type="xsd:string">AnonymousModule</ Setting> </Setting> </Setting> </Setting>`  For more information about editing the `oam-config.xml` file, see Updating OAM Configuration in *Administering Oracle Access Management*. **Note:** Changes are reflected only on Managed Server restarts.

Table 1-5 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Base Bug Number	Description of the Problem
31641787	OUD ATTRIBUTE RESETPWD:TRUE CAUSES AUTHN FAILURE FOR USERAUTHENTICATIONPLUGIN **Note:** You can allow authentication for Oracle Unified Directory password policy attribute `RESETPWD=true` by adding the following attribute to the `oam-config.xml` file under the configured user identity store: `<Setting Name="checkPwdPolicyWarning" Type="xsd:boolean">false</Setting>`
31650595	UNABLE TO START INTERNAL STAGE PRIMARY
31428183	WEBGATE PROFILE GET CORRUPTED IF ADD PRIMARY/SECONDARY SERVER WITH N+2 INDEX USING WEBGATE TEMPLATE.
31039212	GLOBAL LOGOUT NOT CLEARING SESSION
31857424	Fix for Bug 31857424
31744937	REST API:OTP:CREATEOTP & VALIDATEOTP FLOWS NEEDS TO BE FIXED
29154366	OAM-OSB INTEGRATION USING OAUTH2 NOT WORKING
31638527	NULL POINTER EXCEPTION WITH PASSWORD MANAGEMENT DISABLED
28562000	PREAUTHENTICATION RULE TO DENY ACCESS DISPLAYS OPERATION ERROR
31728627	CONCURRENCY ISSUES IN SecurityConfig/ TrustedInputs INITIALIZATION.

Table 1-5 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Base Bug Number	Description of the Problem
31595758	SOME SAML ATTRIBUTES GET MAPPED TO WRONG AVALUES AFTER SAML RESPONSE WITH OAM 12C
31741829	STUCK THREADS IN ORACLE.SECURITY.FED.SECURITY.UTIL.CERTRETRIEVALUTILS.GETSIGNINGCERT IN SAML LOGIN FLOWS
31763785	12CP4 - SESSION_ID IS NOT PRESENT AS PART OF THE CLAIMS IN THE ACCESS TOKEN GENERATED USING SSO LINK FLOW
31526660	THE HEADER IS NOT FOUND FOR SAML MULTI-VALUED RESPONSE VARIABLE
31662739	SESSION LINK TOKEN CANNOT BE USED AS FED ATTRIBUTE
31494411	MULTIPLE INVALID OTP ATTEMPTS DOES NOT LOCK USER OR STOP WRONG OTP ATTEMPTS For more information, see `Doc ID 2743304.1` at https://support.oracle.com.
30991309	DCC TUNNELING UNSOLICITED POST BROKEN IN 12C PS4
24485240	ADDATTRIBUTESTOFEDATTRIBUTES FAILED IF FED SESSION EXISTS

Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Applying this bundle patch resolves the issues listed in the following table:

Table 1-6 Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
31666896	OAM AUTHENTICATION REST API
31516886	USERS CAN'T VIEW APPLICATION DOMAINS IF OAMCONSOLE IS PROTECTED BY WEBGATE
31753451	ERROR WHEN RUNNING WLST COMMAND SETSPPARTNERATTRIBUTEVALUEFILTER
28296759	FORCE PASSWORD RESET NOT WORKING WITH BASIC METHOD AND FORM CACHETYPE
25853168	AFTER UPGRADE TO R12 ONE/FEW CURL COMMAND FOR FEDERATION IS NOT WORKING
29058490	OAM OIM INTEGRATION - LOGIN LOOP AFTER THE USER IS UNLOCKED
27566767	ENH 27566767 - BACKWARD COMPATIBILITY : WITH OAM AS IDP PROVIDE ATTRIBUTE MAPPINGS AND FILTERS IN OAM 12C LIKE OIF 11G
31111719	12CPS4:BP02:ERROR POP UPS ON OAMCONSOLE UI

Table 1-6 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
31427426	SHOWING INVALID PARAMETERS WHILE UPDATING PRIMARY/ SECONDARY SERVER PARAMETERS.
30589288	OIDC SOCIAL LOGIN FAILS DUE TO BLOCKURLS SECURITY CONFIGURATION
30804658	WIN2012R2: NEED TO HANDLE SQL VIOLATION AT ADMIN SERVER BOOTSTRAP
31196076	IPFPSWD.JSP IS THROWING SYSTEM ERROR
26565827	AWS ROLE MAPPING ATTRIBUTE SUPPORT
31186283	ESCAPE CHARACTERS ADDED WHEN CREATING OAUTH TOKEN
31555915	SPECIAL CHARS ON PASSWORD DOES NOT AUTHENTICATE AFTER UPGRADE TO 12.2.1.4
28040138	ORACLE ACCESS MANAGER OPERATION ERROR WHEN AUTHZ POLICY SUCCESSURL IS CONFIGURED
31501282	OAM SYSTEM ERROR ON FORCE PASSWORD CHANGE AFTER APPLYING 12.2.1.3.191201 (BP07)
23096690	PUMA - PERFORMANCE ISSUES SEEN IN APS SYNC-ADD/UPDATE WEBGATE

Table 1-6 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
31038100	ADVANCED RULE PARSING RETURNS UNEXPECTED RESULT FOR ATTRIBUTE EVALUATION

Note:

You must add the user attribute, used in advance rule, as a SYSTEM property where the attribute value is optional.

1. Open `$OAM_DOMAIN/bin/setDomainEnv.sh`.
2. Add `EXTRA_JAVA_PROPERTIES` as shown:

```
EXTRA_JAVA_PROPERTIES="-
Doam.rule.userAttr=<userAtt
r1>::<attrValue>,
<userAttr2>::<attrValue>
${EXTRA_JAVA_PROPERTIES}"

export
EXTRA_JAVA_PROPERTIES
```

For example:

```
EXTRA_JAVA_PROPERTIES="-
Doam.rule.userAttr=description:
:NULL_VALUE
     ${EXTRA_JAVA_PROPERTIES}"

export EXTRA_JAVA_PROPERTIES
```

31289851	OAUTH/OIDC APPROVAL WORKS WHEN NO SESSION FOUND
31337500	OAM MT STUCK THREADS AND HIGH CPU - UIDMX0113
30235925	OAM SESSION SUPPORTS ONLY 40 STRING TYPE PROPERTIES
31068961	ORA-01461: CAN BIND A LONG VALUE ONLY FOR INSERT INTO A LONG COLUMN
28855754	12.2.1.3 OUD PASSWORD POLICY ATTRIBUTE RESETPWD SET TO TRUE CAUSES AUTHN FAILURE
29120924	AMRUNTIMEEXCEPTION:INVALID SETTINGS FOR FORWARD WHEN INTEGRATING DUO PLUGIN
27963081	LDAP RESPONSE READ TIMED OUT - ON IDSTORE CREATION, IF "SEARCH BASE" IS "HUGE"

Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Applying this bundle patch resolves the issues listed in the following table:

Table 1-7 Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
31065568	INTERIM FIX : NEED TO MAKE SURE ALL COOKIES ISSUE BY OAM11G & 12C CONTAIN SAMESITE=NONE
31465732	OAMS.OAM_RESOURCE_URL WARNING MESSAGES STILL DISPLAY IN OAM LOGS WITH FIX 30053037
30053037	OAMS.OAM_RESOURCE_URL WARNING MESSAGES IN OAM LOGS
31510690	PASSWORDRESETREQUESTS REST END POINT THROWS INTERNAL SERVER ERROR.
31508059	INVALID SESSION CONTROL PARAMETERS
30622957	X509 RFC (SECURITY): OAM AUTHN WITH EXTENDEDKEYUSAGE
31366419	UPDATE VALIDATE ENDPOINT TO WORK WITH POST
31413189	MODIFY MDC SESSION CONTROL API FAILES WITH MDC NOT ENABLED ERROR
31419785	THE OAMCUSTOMPAGES.WAR IS NOT DEPLOYABLE.
30953737	WLS ADMIN SERVER LOG FILE AFTER APPLYING AN OAM BUNDLE PATCH THE FOLLOWING WARNING IS NOW SEEN - SOFTLOCK IS ENABLED BUT IS NOT RECOMMENDED SETTING IN PRODUCTION ENVIRONMENT **Note:** To understand how to run the script for disabling/enabling softlock, refer to **readme.txt** in the following directory: `$MW_HOME/idm/oam/server/wlst/scripts/utilities/`
31110638	OAM 12.2.1.4 APR20 BP - IMPORTPOLICY WLST FUNCTION TAKING VERY LONG TIME TO IMPORT POLICIES
29883498	OAM/MDC ISSUE: INVALID SIMPLE MODE ARTIFACTS

Table 1-7 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
30669352	AUTHORIZATION RESPONSE NOT RETURNED FOR AUTHORIZATION FAILURE
30748479	CLIENT IP NOT CAPTURED IN AUDIT.LOG FOR REST CALLS
30406633	GETTING NOT_FOUND WHILE FETCHING ATTRIBUTE FOR SAML RESPONSE HEADER
30762860	Fix for Bug 30762860
31000954	12CPS4 : FEDERATION USES LOCAL IN MEMORY STORE
30120631	SMS OTP PAGE REFRESH
30911495	TWO FACTOR AUTHENTICATION ENTRY TEXTBOX DOES NOT GAIN FOCUS IF THERE IS ONLY ONE OPTION FOR 2ND FACTOR AUTHENTICATION
30628496	UNABLE TO MODIFY PRIMARY/SECONDARY SERVER DATA USING CREATEWEBGATETEMPLATE SYNTAX
30831364	HTTP 405 ON WNA CRED COLLECT ENDPOINT EVEN THOUGH ENDPOINT NOT IN BLOCKURLS LIST
30771422	ADVANCED RULE PARSING FAILS FOR MAP PARAMETERS (USER.USERMAP, REQUEST.REQUESTMAP
30882267	OAM CUSTOM PAGES LOGIN.JSP IS NOT WORKING IN OAM 12.2.1.4
28108712	MODIFY MDC SESSION CONTROL REST API FAILS
29715441	OAM: USERINFO REST CALL DOES NOT RETURN CORRECT VALUE OF TELEPHONENUMBER FOR LDAP PROVIDER OUD

Note:

See also the note `Oracle Access Manager (OAM) "Invalid rule condition" Error On Advanced Rules (Doc ID 2664614.1)` at https://support.oracle.com .

Table 1-7 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
30832165	FEDERATION: FEDSTS-10202: COULD NOT RETRIEVE MDC DATA FROM CLUSTER
30793308	OAM IDP: SYSTEM ERRORS SEEN INTERMITTENTLY DURING FEDERATION LOGOUT
30355996	OAM SESSION API RETURN HTTP 500 ERROR WITH CEST TIMEZONE

Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Applying this bundle patch resolves the issues listed in the following table:

Table 1-8 Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Base Bug Number	Description of the Problem
30805180	OAM Snapshot Tool
30805164	OAUTH CONSENT LIFECYCLE MANAGMENT AND MDC SUPPORT
30805154	OAUTH JUST IN TIME /JIT PROVISIONING
30820170	AUTHORIZATION ERROR WITH USER MEMBER LARGE NUMBER OF GROUP
30792754	MDC ENV. CUSTOM ATTRIBUTES ARE NOT INCLUDED IN ACCESS TOKEN
21391069	NEED TO LOG AUTHENTICATION FAILURE AUDIT LOG FROM CUSTOM PLUGIN
29717855	SAML LOGOUT NOT WORKING IF OLD FED SESSIONS EXIST IN DB
29240849	NEED TO LOG ADDITIONAL AUTHENTICATION FAILURE FOR AUDIT LOG FROM CUSTOM PLUGIN
30634571	12C OAUTH AUDIT RECORDS RETURN NULL VALUES FOR OAUTHTOKENVALIDATE EVENTS
30571576	K8S : OAM_ADMIN AND OAM_SERVER APPLICATION DEPLOYMENT FAILED K8S CLUSTER
29783271	UPDATE OF OUD DETAILS DELETES CONFIG ATTRIBUTE ENTRY ADDED FROM OAM-CONFIG.XML
29885236	ENABLED MULTIVALUEGROUPS SP USE $USER.GROUPS TWICE IN A FED SP ATTRIBUTE PROFILE
30134427	Fix for Bug 30134427
30169956	OAUTH PASSWORD GRANT TYPE CAN ONLY USE NON-PLUGIN LDAP MODULE FOR AUTHENTICATION

Table 1-8 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Base Bug Number	Description of the Problem
30213267	DCC WEBGATE TUNNELING FOR ADF CUSTOM LOGIN PAGE NOT WORKING This fix enables tunneling for custom pages using chunked transfer-encoding. It also provides a way to specify the read-timeout on connections used to fetch custom pages from managed server using the Webgate's user-defined parameter `tunnelingDCCReadTimeout`. Specify the `tunnelingDCCReadTimeout` in seconds, for example, `tunnelingDCCReadTimeout=30`. **Note:** When specifying `tunnelingDCCReadTimeout`, you must also increase `aaaTimeoutThreshold` accordingly.
30460435	DCC TUNNELING WHITELIST CAN NOT BE DISABLED USING ENABLEWHITELISTVALIDATIONDCCTUNNELING CONFIG
30426370	OAM 12.2.1.4:DOWNLOADACCESSARTIFACTS: SEVERE:REQUEST TO PROCESS ARTIFACTS FAILED
30468914	OAM DOES NOT SUPPORT HOLDER OF KEY PROFILE.
30069618	OAMAGENT-02077: AUTHN TOKEN IS EITHER NULL OR INVALID

Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

Applying this bundle patch resolves the issues listed in the following table:

Table 1-9 Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

Base Bug Number	Description of the Problem
26679791	FIX FOR BUG 25898731 IS FAILING IN OAM 11.1.2.3.171017BP 26540179
30389257	TWO FACTOR AUTHENTICATION ENTRY TEXTBOX DOES NOT GAIN FOCUS

Table 1-9 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

Base Bug Number	Description of the Problem
30311080	OIGOAMINTEGRATION.SH - CONFIGURESSOINTEGRATION THROWS UNMARSHAL EXCEPTION IN FRESH 12CPS4 ENV
30156706	OAM ADMIN SERVER START FAILS DUE TO FAIL TO CREATE OAM-CONFIG.XML FROM DBSTORE
29771448	% CHAR IN PASSWORD USED TO GENERATE OAUTH ACCESS TOKEN IS TRANSLATED TO ASCII
30144617	ISSUE ON CHANGE IN BEHAVIOR IN RETURNING ERRORCODE AFTER APPLYING PATCH 29918603
29482858	OAM 11G ASDK INTERMITTENTLY THROWING ERROR WHILE CREATING OBSSOCOOKIE
29541818	ER TO ADDRESSING ADDITIONAL USE CASES OF OAUTH AND JSON IN OAM 12C
29837657	OAM DOES SUBTREE SEARCH TO VALIDATE IDSTORE CREATION
29290091	WRONG SELECT IN ADMIN STARTUP LOGS
30156607	DIAG: ADD MORE LOGS IN AMKEYSTORE VALIDATION FLOW TO IDENTIFY CONFIG THAT CAUSES TO FAIL TO START ADMIN SERVER
30243111	DIAG: REQUIRE LOGS IN DEFAULT KEYSTORE BOOTSTRAPPING FLOW TO IDENTIFY CONFIG MISSING/CORRUPTION ISSUE
30180492	OCI FEDERATION WITH ORACLE ACCESS MANAGER IS NOT WORKING AS EXPECTED
30363797	OAM11GR2PS3 : WNA_DCC MODULE IS FAILING WITH SECURITY BUG FIX :25963019
29649734	12.2.1.3.180904 (BP04) ACCESS SERVER RETURNS JSON KEY AND NOT P7B LIKE DOCUMENT
30062772	FEDERATION BP18 CAUSES LOGOUT END_URL TO BE CONVERTED TO LOWER CASE IN FED LOGOU
30176378	ERRORS IN OAM SERVER LOGS AFTER RUNNING WLST COMMAND DISABLESKIPAUTHNRULEEVAL()
30267123	UNABLE TO LOGIN FROM MULTIPLE TABS AFTER LOGGING IN FROM A TAB.

Known Issues and Workarounds

For known issues and workarounds refer to My Oracle Support Document 2602696.1 at https://support.oracle.com