

Oracle Access Management Bundle Patch Readme

This document describes OAM Bundle Patch 12.2.1.4.201201.

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 12.2.1.4.201201](#)
- [New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200909](#)
- [New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200629](#)
- [New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200327](#)
- [Understanding Bundle Patches](#)
- [Recommendations](#)
- [Bundle Patch Requirements](#)
- [Applying the Bundle Patch](#)
- [Removing the Bundle Patch](#)
- [Resolved Issues](#)
- [Known Issues and Workarounds](#)

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 \(Doc ID 2687940.1\)](https://support.oracle.com) at <https://support.oracle.com>.
- See also the note [Oracle Access Manager \(OAM\): Impact Of SameSite Attribute Semantics \(Doc ID 2634852.1\)](https://support.oracle.com) 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*.

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 help 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 Mechanism \(Opatch\)](#)
- [Applying the OAM Bundle Patch](#)
- [Recovering From a Failed Bundle Patch Application](#)

Note:

Oracle recommends that you always install the latest Bundle Patch.

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 (version 13.9.4.2.5 or higher) 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 earlier than 13.9.4.2.5. If so, download the latest 13.9.4.2.5 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 `p32217874_122140_Generic.zip`
2. Unzip the patch zip file into the `PATCH_TOP`.

```
$ unzip -d PATCH_TOP p32217874_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 p32217874_122140_Generic.zip
```

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

```
$ cd PATCH_TOP/32217874
```

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).

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 `Opatch 13.9.4.2.5` for rollback. If older versions of the Opatch is used for rollback, the following fail message is displayed:

```
C:\Users\\Downloads\p32217874_122140_Generic\32217874
>c:\Oracle\oam12214\OPatch\opatch rollback -id 32217874
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/32217874`
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 32217874`
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 12.2.1.4.201201](#)
- [Resolved Issues in OAM Bundle Patch 12.2.1.4.200909](#)
- [Resolved Issues in OAM Bundle Patch 12.2.1.4.200629](#)
- [Resolved Issues in OAM Bundle Patch 12.2.1.4.200327](#)
- [Resolved Issues in OAM Bundle Patch 12.2.1.4.191223](#)

Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

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

Table 1-1 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 <code>SessionMustBeAnchoredToDataCenterServicingUser</code> must be set to <code>false</code> 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 |

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

| Base Bug Number | Description of the Problem |
|-----------------|--|
| 31734489 | ERROR MESSAGE WHEN USER HAS EXCEEDED THE MAXIMUM NUMBER OF ALLOWED SESSIONS |
| 31098504 | <p data-bbox="777 422 1365 478">FEATURE TO CONFIGURE THE ANONYMOUS USER ACCOUNT NAME</p> <p data-bbox="777 480 1365 594">You can configure username in the anonymous user session by modifying the anonymousUserName in the oam-config.xml file under AnonymousModules. For example:</p> <pre data-bbox="777 667 1292 1171"> <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> </pre> <p data-bbox="777 1224 1365 1312">For more information about editing the oam-config.xml file, see Updating OAM Configuration in Administering Oracle Access Management.</p> |

 **Note:**

Changes are reflected only on Managed Server restarts.

Table 1-1 (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 |
| | <div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>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:</p> <pre data-bbox="1141 961 1325 1178" style="font-family: monospace;"> <Setting Name="checkPwdPolicyWarning" Type="xsd:boolean">false</Setting> </pre> </div> |
| 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 1-1 (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.CERTRETRI EVALUTILS.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 1-2 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 SETSPARTNERATTRIBUTEVALUEFILTER |
| 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 1-2 (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 1-2 (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 |
| | <div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>You must add the user attribute, used in advance rule, as a SYSTEM property where the attribute value is optional.</p> <ol style="list-style-type: none"> 1. Open \$OAM_DOMAIN/bin/setDomainEnv.sh. 2. Add EXTRA_JAVA_PROPERTIES as shown: <pre>EXTRA_JAVA_PROPERTIES="- Doam.rule.userAttr=<userAttr1>::<attrValue>, <userAttr2>::<attrValue> \${EXTRA_JAVA_PROPERTIES}" export EXTRA_JAVA_PROPERTIES</pre> <p>For example:</p> <pre>EXTRA_JAVA_PROPERTIES="- Doam.rule.userAttr=description: :NULL_VALUE \${EXTRA_JAVA_PROPERTIES}" export EXTRA_JAVA_PROPERTIES</pre> </div> |
| 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 1-3 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 FAILS 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 |
| 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 |

 **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/

Table 1-3 (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 1-3 (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 1-4 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 1-4 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

| Base Bug Number | Description of the Problem |
|-----------------|---|
| 30213267 | <p>DCC WEBGATE TUNNELING FOR ADF CUSTOM LOGIN PAGE NOT WORKING</p> <p>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.</p> <p>Specify the tunnelingDCCReadTimeout in seconds, for example, tunnelingDCCReadTimeout=30.</p> |
| | <div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>When specifying tunnelingDCCReadTimeout, you must also increase aaaTimeoutThres hold accordingly.</p> </div> |
| 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 1-5 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 1-5 (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 OBSSOCOKIE |
| 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>

Oracle® Fusion Middleware Oracle Access Management Bundle Patch Readme, OAM Bundle Patch 12.2.1.4.201201 Generic for all Server Platforms
F37772-01

Copyright © 2021, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.