Oracle® Fusion Middleware

Oracle Access Management Bundle Patch Readme

OAM BUNDLE PATCH 12.2.1.3.220113 Generic for all Server Platforms

F51340-01

January 2022

Oracle Access Management Bundle Patch Readme

This document describes OAM BUNDLE PATCH 12.2.1.3.220113

For issues documented after the release of this OAM BUNDLE PATCH 12.2.1.3.220113, see My Oracle Support Document 2568304.1, Oracle Fusion Middleware 12.2.1.3.0 Known Issues (Doc ID 2568304.1)

This document requires a base installation of Oracle Access Management 12c Patch Set 3 (12.2.1.3.0). This supersedes the documentation that accompanies Oracle Access Management 12c Patch Set 3 (12.2.1.3.0), it contains the following sections:

- New Features and Enhancements in OAM Bundle Patch 12.2.1.3.210915
- New Features and Enhancements in OAM Bundle Patch 12.2.1.3.201201
- New Features and Enhancements in OAM Bundle Patch 12.2.1.3.200908
- New Features and Enhancements in OAM Bundle Patch 12.2.1.3.200629
- 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 12.2.1.3.210915

Oracle Access Management 12.2.1.3.210915 BP includes the following new features and enhancements:

- **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`.

New Features and Enhancements in OAM Bundle Patch 12.2.1.3.201201

Oracle Access Management 12.2.1.3.201201 BP includes the following new features and enhancements:

- **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 12.2.1.3.200908

Oracle Access Management 12.2.1.3.200908 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 12.2.1.3.200629

Oracle Access Management 12.2.1.3.200629 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.

Understanding Bundle Patches

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

- [Bundle Patch](#)
- [Patch Set](#)

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
- 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 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:**
>
> Patching Your Environment Using OPatch

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 excecutables 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 p33752617_122130_Generic.zip
2. Unzip the patch zip file into the PATCH_TOP.

```
$ unzip -d PATCH_TOP p33752617_122130_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 p33752617_122130_Generic.zip
```

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

```
$ cd PATCH_TOP/33752617
```

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 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\p33752617_122130_Generic\33752
> 617
> >c:\Oracle\oam12213\OPatch\opatch rollback -id 33752617
> 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/33752617`

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 33752617
```

> **✎ Note:**
>
> - To rollback the patch completely, remove the below two entries from `oam-config.xml` file using the `config-utility` tool (Doc : 2310234.1):
>
>   - `<Setting Name="PolicyCacheComponent" Type="htf:map"> ........ </Setting>`
>
>   - `<Setting Name="PolicyCacheManagementAPI" Type="htf:map"> ...... </Setting>`

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 12.2.1.3.220113
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210915
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210701
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210324
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200908
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200629
- Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.0 (ID:191201.0123.S)
- Resolved Issues in 12.2.1.3.190609
- Resolved Issues in 12.2.1.3.181213
- Resolved Issues in 12.2.1.3.180904
- Resolved Issues in 12.2.1.3.180706
- Resolved Issues in 12.2.1.3.180414
- Resolved Issues in 12.2.1.3.171121

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.220113

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

Table 1-1   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.220113

Base Bug Number	Description of the Problem
33533200	AUTHZ CALL FAILS WHEN RDN HAS SPECIAL CHARACTER **✐ Note:** This bug is dependent on libovd patch 33626315
33518405	Fix for Bug 33518405
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
33391677	FEDERATED USER HAVING \ IS SENDING \5C\ TO LIBOVD WITH FILTERESCAPE VALUE TRUE **✐ Note:** This bug is dependent on libovd patch 33626315
33142450	USER STILL RETURNED TO THE URL EVEN WITH RETURNURLVALIDATIONENABLED

Table 1-1 (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.220113

Base Bug Number	Description of the Problem
33098826	UNSOLICITED LOGIN FLOW BREAKS WITH PASSWORD POLICY WITH SFA FLOW

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210915

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

Table 1-2 Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210915

Base Bug Number	Description of the Problem
33122045	ACCESS MANAGER KEYSTORE VALIDATION FOR SSL AND UDM PASSWORD SHOULD BE ENABLED FOR UPGRADE

> **Note:**
>
> To enable SSL configuration validation when upgrading OAM to 12.2.1.3.0, set the following `EXTRA_JAVA_PROPERTIES` in `setDomainEnv.sh`.
>
> `-Doracle.oam.install.SimpleModeValidationEnable=true`

Base Bug Number	Description of the Problem
33055065	FEDERATION NOT WORKING AFTER ACCESSING OAM PROTECTED PAGE
33074398	ISSUE WITH APNS PATCH 32625905: SOUND MISSING
32807465	DELETING IDENTITY PROVIDER CANNOT REPLICATE TO CLONE SERVER FROM MASTER
32920684	IMPORTPOLICYDELTA FAILS TO IMPORT ADVANCED AUTHENTICATION RULES
32482754	INCREASE OAUTH ACCESS TOKEN MAXIMUM SIZE TO MORE THAN 5000 CHARACTERS

Table 1-2   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210915

Base Bug Number	Description of the Problem
32879893	INTERMITTENT ERRORS IN OAM CONSOLE PREVENT VIEWING & UPDATING POLICY OBJECTS
32543656	OAM 11G (SP) SHOULD END THE LOCAL SESSION WHEN RECEIVING SOAP LOGOUT REQUEST
32568653	12 VERSION : ACCESSSERVERCONFIGPROXY PORT CHANGING 5576 TO 5575 RESTARTADMIN
32826737	TEST CONNECTION FOR LDAP IN OAM CONSOLE FAILS FOR TLS 1.2 ON IBM AIX
32976735	EBS APPSLOGIN FAILS WHEN USING OAM WITH OUD AS BACKEND LDAP ON AIX WITH TLS 1.2 ONLY **Note:** This bug is dependent on libovd patch 27231407
33086248	OAM READINESS CHECK: THE MESSAGE DISPLAYED TWICE FOR .OAMKEYSTORE ON UPGRADE UI
32953208	OAM OPENID CONNECT LOGOUT DOES NOT FORWARD STATE PARAMETER TO POST_LOGOUT_REDIRE
32933119	API /OAUTH2/REST/SECURITY DO NOT WORKING ERROR 406
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`.

Table 1-2   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210915

Base Bug Number	Description of the Problem
31843528	ASSERTION HAS AN ADVICE ELEMENT THAT CONTAINS AN ENCRYPTED FIELD THAT FAILS OAM
32828842	OIDC-PIREAN INTEGRATION - NOT A VALID JWT TOKEN
32734517	NOT ABLE TO UPDATE THE AUTHNSCHEMELEVEL FROM 5 TO 2 FOR X509 USING CURL
32701831	REDIRECT LOOP USING INITIAL_COMMAND=NONE AFTER APPLICATION DOMAIN IDLE TIMEOUT
32655233	LIBOVD 12C SPECIAL CHARACTER IN USERNAME FAILS TO LOCATE USER IN LDAP

> ✏ **Note:**
>
> This bug is dependent on libovd patch 32305678

Base Bug Number	Description of the Problem
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
27584970	CAPACITY CONSTRAINT IN WEBLOGIC-APPLICATION.XML CAUSING PERFORMANCE IMPACT
27582324	POST DATA RESTORATION FAILS WHEN OBRAR.CGI USES GET METHOD TO RETRIEVE DATA .

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210701

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

Table 1-3   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210701

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
32428227	OAM_ADMIN DEPLOYMENT HAS FAILED

ORACLE®

Table 1-3   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210701

Base Bug Number	Description of the Problem
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=<clientName>' \--header 'Authorization: Basic d2VibG9naWM6V2VsY29tZTE=' \--header 'Accept: application/json' \```

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

Table 1-3   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210701

Base Bug Number	Description of the Problem
32614444	OIDC-PIREAN UNEXPECTED EXCEPTION ENCOUNTERED WHILE PROCESSING JOSE OBJECT
31629661	ASDK FAILS TO CONNECT TO RUNNING OAM SERVER.
32507312	ISSUE ACCESSING /OAMFED/USER/SLOOAM11G? ID=OAM11G&TYPE=3
32376345	NEED ALTERNATE SOLUTION FOR 31186283 TO REDUCE EXTRA CALL TO OAM ENDPOINT
32440706	ERROR WHEN SUCCESSURL CONTAIN PARAMETER STARTING WITH INT
32153972	SIGNATURE VALIDATION FAILED OPENIDCONNECTPLUGIN CONFIGURATION.
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.

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210324

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

Table 1-4   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210324

Base Bug Number	Description of the Problem
32632139	OAM 12CPS3: FIX FOR BUG #32055280 IS FAILING
32380255	IOS PUSH NOTIFICATIONS PORTS 2195 AND 2196 ARE DEPRECATED FROM MARCH
32250953	INTERMITTENT LOGIN ISSUE WITH INTERNAL OAM ADC ENVIRONMENT
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.
32367518	ADD DOCID IN THE UR3 OAM READINESS CHECK
32367473	OAM READINESS CHECK IS NOT ADDED FOR COEXISTMODE AND ISCOEXISTMODEWITH10G

Table 1-4 (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.210324

Base Bug Number	Description of the Problem
32367429	OAM READINESS CHECK: NO VALIDATION IF KEYSTORE FILES NOT PRESENT UNDER FMWCONFIG
30352121	NEED POSSIBILITY TO FILTER USER GROUPS SENT IN SAML RESPONSE IN FEDERATED ENV.
32367489	OAM READINESS CHECK : INCORRECT ERROR MESSAGE IN READINESS CHECK UI FOR READINESS CHECK FAILURE USE CASE
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
31750371	SYSYEM ERROR AFTER REACHING INVALID OTP MAXATTEMPTS IN STANDALONE ENV
32136382	NULLPOINTEREXCEPTION AFTER ADDING "-DORACLE.OAM.ENABLEEXTRASAMLATTR=TRUE"
31900502	OAM12C - FORGOT PASSWORD WITH ONE-TIME PASSWORD DOESN'T WORK WITH SERVERREQUESTCACHETYPE FORM
31830597	OAUTH : ACCESS AND REFRESH TOKEN EXPIRY TIME NOT SET CORRECTLY
31822228	MFA FAILS WHEN ANONYMOUS SESSION EXISTS

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201

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

Table 1-5 Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201

Base Bug Number	Description of the Problem
32081498	ENHANCE THE OAM READINESS CHECK TO IDENTIFY ANY EXISTING ISSUE BEFORE UPGRADE.

Table 1-5   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201

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.

31832371	REQUESTING OPTION TO LEAVE OAUTH_TOKEN RESPONSE UNSET WITH ER 29541818
31650595	UNABLE TO START INTERNAL STAGE PRIMARY
31428183	WEBGATE PROFILE GET CORRUPTED IF ADD PRIMARY/SECONDARY SERVER WITH N+2 INDEX USING WEBGATE TEMPLATE.
31744937	REST API:OTP:CREATEOTP & VALIDATEOTP FLOWS NEEDS TO BE FIXED

Table 1-5   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201

Base Bug Number	Description of the Problem
31638527	NULL POINTER EXCEPTION WITH PASSWORD MANAGEMENT DISABLED
31766587	OAM 12C-OPEN ID CONNECT-NONCE CLAIM MISSING IN TOKEN
31734489	ERROR MESSAGE WHEN USER HAS EXCEEDED THE MAXIMUM NUMBER OF ALLOWED SESSIONS
31778001	Fix for Bug 31778001
31728627	CONCURRENCY ISSUES IN SecurityConfig/ TrustedInputs INITIALIZATION.
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
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="checkPw
> dPolicyWarnin
> g"
> Type="xsd:boo
> lean">false</
> Setting>
> ```

31662739	SESSION LINK TOKEN CANNOT BE USED AS FED ATTRIBUTE

Table 1-5   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.201201

Base Bug Number	Description of the Problem
31516886	USERS CAN'T VIEW APPLICATION DOMAINS IF OAMCONSOLE IS PROTECTED BY WEBGATE
31469921	MULTI VALUE ATTRIBUTES ARE NOT RETURNING VALUE FROM FEDERATION AT 12C
31526660	THE HEADER IS NOT FOUND FOR SAML MULTI-VALUED RESPONSE VARIABLE
30503494	AFTER AUTHENTICATION FAILURE USER DOES NOT REDIRECT TO FAILURE URL
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.
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.
30792754	MDC ENV. CUSTOM ATTRIBUTES ARE NOT INCLUDED IN ACCESS TOKEN
28946202	OAM AUDITING NOT CAPTURING IAU_INITIATOR FOR FAILED AUTHENTICATION ATTEMPTS

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200908

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

Table 1-6   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200908

Base Bug Number	Description of the Problem
27566767	ENH 27566767 - BACKWARD COMPATIBILITY : WITH OAM AS IDP PROVIDE ATTRIBUTE MAPPINGS AND FILTERS IN OAM 12C LIKE OIF 11G

Table 1-6   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200908

Base Bug Number	Description of the Problem
31427426	SHOWING INVALID PARAMETERS WHILE UPDATING PRIMARY/SECONDARY SERVER PARAMETERS.
30804658	WIN2012R2: NEED TO HANDLE SQL VIOLATION AT ADMIN SERVER BOOTSTRAP
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
31501282	OAM SYSTEM ERROR ON FORCE PASSWORD CHANGE AFTER APPLYING 12.2.1.3.191201 (BP07)
31196076	IPFPSWD.JSP IS THROWING SYSTEM ERROR
31337500	OAM MT STUCK THREADS AND HIGH CPU - UIDMX0113
31366419	UPDATE VALIDATE ENDPOINT TO WORK WITH POST
31176394	OAMCUSTOMPAGES.WAR MISSING SOME PAGES/ FILES
30831364	HTTP 405 ON WNA CRED COLLECT ENDPOINT EVEN THOUGH ENDPOINT NOT IN BLOCKURLS LIST
30134427	Fix for Bug 30134427
29058490	OAM OIM INTEGRATION - LOGIN LOOP AFTER THE USER IS UNLOCKED
26945293	INCORRECT ERROR MESSAGE DISPLAYED FOR AD.

> **✎ Note:**
>
> This bug is dependent on libovd patch 26819748

29783271	UPDATE OF OUD DETAILS DELETES CONFIG ATTRIBUTE ENTRY ADDED FROM OAM-CONFIG.XML
25853168	AFTER UPGRADE TO R12 ONE/FEW CURL COMMAND FOR FEDERATION IS NOT WORKING

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200629

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

Table 1-7   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200629

Base Bug Number	Description of the Problem
31065568	INTERIM FIX : NEED TO MAKE SURE ALL COOKIES ISSUE BY OAM11G & 12C CONTAIN SAMESITE=NONE
31510690	PASSWORDRESETREQUESTS REST END POINT THROWS INTERNAL SERVER ERROR.
31508059	INVALID SESSION CONTROL PARAMETERS
31465732	OAMS.OAM_RESOURCE_URL WARNING MESSAGES STILL DISPLAY IN OAM LOGS WITH FIX 30053037
31413189	MODIFY MDC SESSION CONTROL API FAILES WITH MDC NOT ENABLED ERROR
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_HO ME/idm/oam/ server/wlst/ scripts/ utilities/`

Base Bug Number	Description of the Problem
31089954	DIAG BUG: NEED TO ADD DIAGNOSTICS AROUND DEFAULT-KEYSTORE
31068961	ORA-01461: CAN BIND A LONG VALUE ONLY FOR INSERT INTO A LONG COLUMN
30677281	DIAG: ADD ERROR/WARNING LEVEL LOGGING MESSAGE TO IDENTIFY REDIRECT URLS ARE NOT WHITELISTED.
30762860	Fix for Bug 30762860
30120631	SMS OTP PAGE REFRESH
30748479	CLIENT IP NOT CAPTURED IN AUDIT.LOG FOR REST CALLS
30832165	FEDERATION: FEDSTS-10202: COULD NOT RETRIEVE MDC DATA FROM CLUSTER

Table 1-7 (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200629

Base Bug Number	Description of the Problem
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
30053037	OAMS.OAM_RESOURCE_URL WARNING MESSAGES IN OAM LOGS
30235925	OAM SESSION SUPPORTS ONLY 40 STRING TYPE PROPERTIES
30793308	OAM IDP: SYSTEM ERRORS SEEN INTERMITTENTLY DURING FEDERATION LOGOUT
30820170	AUTHORIZATION ERROR WITH USER MEMBER LARGE NUMBER OF GROUP
30634571	12C OAUTH AUDIT RECORDS RETURN NULL VALUES FOR OAUTHTOKENVALIDATE EVENTS
29883498	OAM/MDC ISSUE: INVALID SIMPLE MODE ARTIFACTS
30669352	AUTHORIZATION RESPONSE NOT RETURNED FOR AUTHORIZATION FAILURE
29885236	ENABLED MULTIVALUEGROUPS SP USE $USER.GROUPS TWICE IN A FED SP ATTRIBUTE PROFILE
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.
30468914	OAM DOES NOT SUPPORT HOLDER OF KEY PROFILE.

Table 1-7   (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.200629

Base Bug Number	Description of the Problem
30355996	OAM SESSION API RETURN HTTP 500 ERROR WITH CEST TIMEZONE
30069618	OAMAGENT-02077: AUTHN TOKEN IS EITHER NULL OR INVALID
30406633	GETTING NOT_FOUND WHILE FETCHING ATTRIBUTE FOR SAML RESPONSE HEADER
30460435	DCC TUNNELING WHITELIST CAN NOT BE DISABLED USING ENABLEWHITELISTVALIDATIONDCCTUNNELING CONFIG
24485240	ADDATTRIBUTESTOFEDATTRIBUTES FAILED IF FED SESSION EXISTS

Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.0 (ID:191201.0123.S)

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

Table 1-8   Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.0 (ID:191201.0123.S)

Base Bug Number	Description of the Problem
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
30180492	OCI FEDERATION WITH ORACLE ACCESS MANAGER IS NOT WORKING AS EXPECTED
30156607	DIAG: ADD MORE LOGS IN AMKEYSTORE VALIDATION FLOW TO IDENTIFY CONFIG THAT CAUSES TO FAIL TO START ADMIN SERVER
29940526	ERROR MESSAGE POP-UP DISPLAYS WHILE CREATING SP/IDP PARTNER
30243111	DIAG: REQUIRE LOGS IN DEFAULT KEYSTORE BOOTSTRAPPING FLOW TO IDENTIFY CONFIG MISSING/CORRUPTION ISSUE
30144617	ISSUE ON CHANGE IN BEHAVIOR IN RETURNING ERRORCODE AFTER APPLYING PATCH 29918603
30363797	OAM11GR2PS3 : WNA_DCC MODULE IS FAILING WITH SECURITY BUG FIX :25963019
30176378	ERRORS IN OAM SERVER LOGS AFTER RUNNING WLST COMMAND DISABLESKIPAUTHNRULEEVAL()
30169956	OAUTH PASSWORD GRANT TYPE CAN ONLY USE NON-PLUGIN LDAP MODULE FOR AUTHENTICATION

Table 1-8 (Cont.) Resolved Issues in OAM BUNDLE PATCH 12.2.1.3.0 (ID:191201.0123.S)

Base Bug Number	Description of the Problem
27767574	STRESS:OAM12C:ERROR WHILE PROCESSING MASTER CONTROLLER IN PBL NULLPOINTEREXCEPT
29154366	OAM-OSB INTEGRATION USING OAUTH2 NOT WORKING
30267123	UNABLE TO LOGIN FROM MULTIPLE TABS AFTER LOGGING IN FROM A TAB.
29541818	ER TO ADDRESSING ADDITIONAL USE CASES OF OAUTH AND JSON IN OAM 12C
30062772	FEDERATION BP18 CAUSES LOGOUT END_URL TO BE CONVERTED TO LOWER CASE IN FED LOGOU
29837657	OAM DOES SUBTREE SEARCH TO VALIDATE IDSTORE CREATION
29993720	FORGOT PASSWORD LINK DISAPPEARS AFTER CHANGING THE LANGUAGE OF THE BROWSER
27036000	OTP CODE PAGE REFRESH
29558937	UPDATEWEBGATETEMPLATETOWEBGATEMAPPING CAUSES ERROR IN ADMINSERVER LOGS
29482858	OAM 11G ASDK INTERMITTENTLY THROWING ERROR WHILE CREATING OBSSOCOOKIE
29664878	OAM 12C OAUTH CERT JWK : EXTEND CERTIFICATE VALIDITY OR RENEW CERTIFICATE
29349299	Fix for Bug 29349299
29874540	AUTHENTICATION ISSUE FOR USER WHO IS MEMBER OF LARGE GROUP AND CONFIGURED MEMBEROF AS PREFETCH ATTRIBUTE
29290091	WRONG SELECT IN ADMIN STARTUP LOGS
28108712	MODIFY MDC SESSION CONTROL REST API FAILS
29233064	Fix for Bug 29233064
29649734	12.2.1.3.180904 (BP04) ACCESS SERVER RETURNS JSON KEY AND NOT P7B LIKE DOCUMENT
29603419	JWT BEARER GRANT FLOW TO GET OAUTH ACCESS TOKEN FROM JWT ASSERTION RESULT ERROR
29463380	FEDERATION MULTIVALUEGROUPS ATTRIBUTE DOES NOT PARSE COMMAS IN GROUP NAMES
28348030	Fix for Bug 28348030
25963019	Fix for Bug 25963019

Resolved Issues in 12.2.1.3.190609

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

Table 1-9   Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
29639271	12C OAUTH - CUSTOM ATTRIBUTES NOT UPDATING IN CLIENT CONFIGURATION
29715441	OAM: USERINFO REST CALL DOES NOT RETURN CORRECT VALUE OF TELEPHONENUMBER FOR LDAP PROVIDER OUD

> ✏️ **Note:**
>
> You can retrieve the telephone number by adding the following attribute to the `oam-config.xml` file under the configured OUD user identity store: `<Setting Name="TELEPHONE_NUMBER_ATTRIBUTE" Type="xsd:string">telephonenumber</Setting>`

Base Bug Number	Description of the Problem
29777410	"SYSTEM ERROR PAGE" CODE IS DISPLAYED DIRECTLY WHEN DCC TUNNELED RESOURCE WITH PASSWORD POLICY IS ACCESSED
29769613	OAM : REST API TO FETCH SESSION DETAILS USING UPDATETIME DOES NOT RETURN CORRECT VALUES
29717855	SAML LOGOUT NOT WORKING IF OLD FED SESSIONS EXIST IN DB
29482228	NEW ACCESS TOKEN FROM REFRESH TOKEN DOES NOT CONTAIN UPDATED USER ATTR VALUE
29425002	LOGIN ISSUE FOR USERS WITH LARGE NUMBER OF GROUP MEMBERSHIPS
29423470	STANDARD OUD PHONE ATTRIBUTE CANNOT BE RETRIEVED IN USERINFO
29305502	LONG NAME IN X509PLUGIN FAILED TO AUTHENTICATE
29244150	SSO BETWEEN TUNNELED DCC AND PLAIN DCC IS BROKEN WHEN APPLIED OAM BP'S 14,15 OR 16

ORACLE®

Table 1-9   (Cont.) Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
29240849	NEED TO LOG ADDITIONAL AUTHENTICATION FAILURE FOR AUDIT LOG FROM CUSTOM PLUGIN
29233897	DIAG: NEED DETAILED DEBUG OUTPUT FOR NPE ON OAUTH CODE
29120924	AMRUNTIMEEXCEPTION:INVALID SETTINGS FOR FORWARD WHEN INTEGRATING DUO PLUGIN
29053141	OAM_REQ_ID COOKIE IS NOT INVALIDATED RESULTING ERROR - BAD REQUEST
29041992	OFUSIONMIDDLEWAREAUDIT->COMMONREPORTS->ACCOUNTMANAGEMENT->DASHBOARD THROW ERROR
29011613	12C:RSA:GETTING SYSTEM ERROR (LOADER CONSTRAINT VOILATION ERR)WHEN ACCESSING RSA RESOURCE
28861117	JAVASCRIPT ERROR THAT DISPLAYMSG() IS UNDEFINED
28855754	12.2.1.3 OUD PASSWORD POLICY ATTRIBUTE RESETPWD SET TO TRUE CAUSES AUTHN FAILURE

> **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>"`

Base Bug Number	Description of the Problem
28833416	PASSWORD POLICY: UNABLE TO SET PASSWORD DICTIONARY FILE

Table 1-9 (Cont.) Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
28811365	SAML LOGOUT NOT WORKING ON DCC TUNELING ON CLUSTER NULLPOINTEREXCEPTION

> **✎ Note:**
>
> An intermittent issue with SAML logout that is seen in cluster environment is fixed. You must enable the stickiness for the Embedded Credential Collector (ECC) and the load balancing router. For Detached Credential Collector (DCC) you must set the `rdbmsasynchronousenabled` value in the `oam-config.xml` file to `false`.

Base Bug Number	Description of the Problem
28753576	UPDATE FIX FOR : FED-18059 USER MISMATCH WITH OAM BP13 AND PATCH 27050584 APPLIED
28728420	OAM-OIM FIRSTLOGIN PAGE IS BLANK, BACKURL CONTAIN HOST IDENTIFIER
28716108	OAM SESSION REST API FAILS WHEN DATES ARE INCLUDED IN SESSION FILTER
28710053	OAM AS SP MUST BE ABLE TO PROCESS A SLO REQUEST FROM A THIRD PARTY IDP
28608117	R2PS3: CREATE WEBGATE TEMPLATE WLST ALLOWING TO CREATE TEMPLATE WITH INVALID PARAMETER
28585170	DASHBOARD FOR AUTHENTICATION AND AUTHORIZATION REPORT CHART IS WRONG

Table 1-9   (Cont.) Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
28562000	PREAUTHENTICATION RULE TO DENY ACCESS DISPLAYS OPERATION ERROR
	Note: This bug has a dependency on WebGate (Bug: 28793688). To resolve the issue for WebGate, request a interim patch from My Oracle Support.
28548575	OAM CANNOT DECODE PROPERLY AN URL WITH TWO QUESTION MARKS
28490555	SESSION REST API FAILS WHEN IDLE SESSIONS FOUND
28308009	OAM 12C OAUTH CLIENT SECRET LOST WHEN UPDATING CLIENT
28244927	12C BP: NEWLY CREATED USER LOGIN GOT ERROR
28240206	WRONG "THE SPECIFIED USER SEARCH BASE IS INVALID" MESSAGE IN OAM CONSOLE
28092100	UNABLE TO UPDATE/MODIFY FAILURE URL OF AUTHENTICATION POLICY USING CURL COMMAND
28004912	STRESS:122131OAM- HIGH CPU (70%) IN OAM OAUTH OIDC STRESS TEST WITH 250 VU LOAD
27977911	NO CUSTOM ATTRIBUTES IN ACCESS TOKEN FOR IMPLICIT GRANT TYPE

Table 1-9   (Cont.) Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
27963081	LDAP RESPONSE READ TIMED OUT - ON IDSTORE CREATION, IF "SEARCH BASE" IS "HUGE" ✎ **Note:** You can use the `com.sun.jndi.ldap.read.timeout` environment property to specify the read timeout for an LDAP operation. The default value is `2000` milliseconds. To increase the JNDI/LDAP read timeout to `15000` milliseconds, add the following attributes in the `setDomainEnv` script file: • `ORACLE_OAM_ JNDILDAPREA DTIMEOUT="1 5000"` • `export ORACLE_OAM_ JNDILDAPREA DTIMEOUT`
27946582	WNA POST FALLBACK IS FAILING AFTER APPLYING BP13
27708019	OAM11.1.2.3 : FEDERATION: LOGOUT SAMLRESPONSE DOES NOT INCLUDE RELAYSTATE.

ORACLE

Table 1-9 (Cont.) Resolved Issues in 12.2.1.3.190609

Base Bug Number	Description of the Problem
27441865	CLIENTSSLKEYSTOREPWD, CLIENTSSLTRUSTSTOREPWD NOT PROPERLY WRITTEN IN OAM-CONFIG

> **✎ Note:**
>
> To resolve the issue, specify STS as the map name (folder) of the credential. For example:
> ```
> createCred(map=
> "STS",
> key="clientsslk
> eystorepwd",
> user="UniqueUse
> rNameCredential
> ",
> password="mypas
> sword",
> desc="identity
> keystore pwd")
> ```

Base Bug Number	Description of the Problem
27343162	Fix for bug 27343162
26866652	THE NULLPOINTEREXCEPTION IS SHOWING IN FORM-FILL APPLICATION IDS PROFILE
25860509	DIAG: ADVANCED RULES NEED THE ABILITY TO CHECK PERFORMANCE OF THE RULE EXECUTION
25659094	DIAG: NEED MORE DETAILS FOR "MISMATCH SHOULD_BE:" ERROR
25541101	/OAM/PAGES/PSWD.JSP NOT WORKING VIA DCC TUNNELLING
25417605	DIAG: "ACTION FAILED DUE TO INCONSISTENT STATUS OF PLUGIN IN DIFF MANAGED SRV"
21391069	NEED TO LOG AUTHENTICATION FAILURE AUDIT LOG FROM CUSTOM PLUGIN

Resolved Issues in 12.2.1.3.181213

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

Base Bug Number	Description of the problem
28772291	OAM LOGIN STOPS WORKING AFTER SETTING SESSION LIFETIME TO 30 DAYS/ 43200 MINUTES

Base Bug Number	Description of the problem
28738544	TRACKING BUG FOR BACKPORTING POLICY CORRUPTION FIX DONE IN 19C - MAIN BRANCH

> ✏️ **Note:**
>
> To rollback this fix completely, remove the below two entries from `oam-config.xml` by using config-utility tool (Doc ID : 2310234.1 in https://support.oracle.com/)
>
> - ```
>   <Setting Name="PolicyCacheComponent" Type="htf:map">
>   ......
>   </Setting>
>   ```
> - ```
>   <Setting Name
>   ```

Base Bug Number	Description of the problem
	="Po licy Cach eMan agem entA PI" Type ="ht f:ma p"> ...... </ Sett ing>
28677784	REVERT THE CHANGES DONE FOR BUG 27132341
28608189	UNABLE TO CONFIGURE DYNAMIC CUSTOM ATTRIBUTE DURING OAUTH CLIENT CREATION
28529484	OAM SENDING DIFFERENT ATTRIBUTE VALUE FROM OID WHICH IS NULL OR NOT AVAILABLE
28528259	WHITELIST COMPARISON IS CASE SENSITIVE FOR HOSTNAME
28487853	OAM HEARTBEAT FAILS AFTER CHANGING TO COOKIE_BASED SESSION

Base Bug Number	Description of the problem
28476106	FEDERATION ATTRIBUTES INCORRECTLY POPULATED FROM MEMBEROF

> **✎ Note:**
>
> This fix has made the`responseSeparator` and `responseEscape` configurable and the configuration is read from the `oam-config.xml` directly. Please use the below wlst command to change the `responseSeparator` and `responseEscapeChar`. For Example:
>
> ```
> configurePolicyResponse(responseSeparator=",",responseEs
> ```

Base Bug Number	Description of the problem
	capeCha r="\\")
28461633	SYSTEMERROR ON FEDERATION-OIM INTEGRATION LOGIN AFTER APPLYING PATCH 27897816
28399922	JWT BEARER FLOW THROWS ERROR ON REQUESTING ACCESS TOKEN WITH OPENID SCOPES
28383964	OAM NOT RECEIVING CLIENT IP ADDRESS AFTER APPLYING THE PATCH: 28177877
28373408	PERSISTENT LOGIN CREATES MULTIPLE SESSIONS WITH NO SOURCE IP
28290015	INCORRECT "/JWKS_URI" ENDPOINT RESPONSE FORMAT
28283068	OAM OIDC THROWS 500 ERROR IN AUTHZ REQUEST HAVING ONLY OPENID RELATED SCOPES
28020400	ERROR WHEN TRY TO REFRESH USING REFRESH_TOKEN
27962269	EXCEPTION WHILE DECRYPTION TOKEN
27791146	CHECKBOXES NOT WORKING ON PASSWORDPOLICY PAGE
27684940	DUTCH TRANSLATION OF PASSWORD POLICY RULES IS INCOMPREHENSIBLE
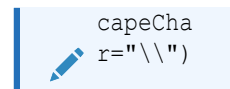
Base Bug Number	Description of the problem
27492853	ADD SUPPORT FOR CUSTOM AUDIT EVENT TYPES FOR FEDERATION

> 📝 **Note:**
>
> Follow the below steps to configure Custom audit events for Federation:
>
> 1. From oam console, set **Audit Preset** filter to **Custom**.
>
> 2. Use WLST `setFedCustomAuditEvents()` and `displayFedCustomAuditEvents()` to configure

Base Bug Number	Description of the problem
	auditing.
	3. Restart servers each time custom events are configured.
27379500	~ IN HEAD OF LOGIN NAME CAUSES SYSTEM ERROR AT AUTOLOGIN AFTER "FORGOT PASSWORD"
27343458	Fix for bug 27343458
26732310	UNABLE TO SEE THE RESOURCES, AUTHRZATION & AUTHNTCTION POLICIES AFTER APPLICATI
23096690	PUMA - PERFORMANCE ISSUES SEEN IN APS SYNC-ADD/UPDATE WEBGATE

Resolved Issues in 12.2.1.3.180904

Base Bug Number	Description of the problem
28541209	OAM 12CPS3: DISPLAYING WRONG ERROR MESSAGE FOR LOCKED USERS
28296759	FORCE PASSWORD RESET NOT WORKING WITH BASIC METHOD AND FORM CACHETYPE
28244683	12C BP: MORE THAN 5 TIMES USING WRONG PWD NOT REDIRECT TO FORGOT PASSWORD

Base Bug Number	Description of the problem
28204062	AUDITOR RELOAD DOESN'T HAPPEN IN OAM 12C WHILE CHANGING FILTER PRESET
	Note: • This bug has a dependency on OPSS October Bundle Patch. Please apply OPSS Bundle Patch 12.2.1.3.181016:28172453 along with OAM Bundle Patch • BI Publisher in standalone mode i.e. with only BIPublisher option while configuring domain is recommended for viewing OAM Reports.
28202816	BP10 ON WEBGATE BREAKS LOGOUT FUNCITONALITY
28132498	EXCEPTION OCCUR WHEN REMOVEWEBGATETEMPLATEPARAMS WHITH NON-EXISTING TEMPLATE
28131039	12C: REMOVE COHERENCE CHECK FROM HEARTBEAT
27931928	AUTHORIZATION BROKEN IN APRIL OAM BP 11.1.2.3.180417 |BP14
27918612	SAML ATTRIBUTE VALUE IS NULL WHEN ONE OF THE USER ATTRIBUTE VALUE IS NULL IN COM
27797404	IMPCONSENT.JSP PAGE IS DOWNLOADED WHEN ACCESSING THROUGH DCC WEBGATE
27614683	OAM INITIATED LOGOUT NOT WORKING & ORA_OSFS_SESSION IS NOT GETTNIG CLEARED

Base Bug Number	Description of the problem
27573288	Fix for Bug 27573288
	Note: This bug fix introduces changes to the following password policy features:
	• Password expiry warning period— This feature is supported only with OAM and OIM integrated scenarios. If there is no OIM integration then OAM authentication will fail during the warning period and the customer has to configure custom authentication plugins to show password expiry warning page and the required handling for the authentication flow.
	The limitation on authentication failure during the password expiry warning period is because of the difference in behavior of different LDAP servers(OID, OUD) when a user tries to authenticate with wrong password during expiry warning period.
	• Password grace login attempts - This configuration will work only if "Password expiry warning period " is not configured. In the first scenario, grace login is not required because user will be forced to change the password during the warning period or after expiry.
27525584	Fix for Bug 27525584
27444036	F5 HEALTH MONITOR GETTING 404 FOR /OAM/SERVER/HEARTBEAT
27417512	Fix for Bug 27417512
27314441	OAM LOGIN FAILS WITH OAMSSA-20144 IF THE USER IN OID WITHIN GRACE LOGINS
27189773	OIDC: ACCESS TOKEN STILL VALID WHEN REM_EXP<0
25417176	FEDERATION: AUTO PROVISION TO LDAP FROM IDP SAML ASSERTION FAILS
23133385	Fix for Bug 23133385

Resolved Issues in 12.2.1.3.180706

Base Bug Number	Description of the problem
28138969	ASDK ERROR FOR URL ENCODED TOKEN AFTER 28027669 FIX **Note:** OAM ASDK —`oamasdk-api.jar` is available in `$ORACLE_HOME/common/lib` directory, copy the same to the host where the application using ASDK is deployed.
28027669	ASDK API FIX FOR BUG:27161546
27931041	COMPATIBILITY FIX & OAM11.1.2.3.180417:SYS ERR FOR 10G WG FOR RSRC %26.HTML
27802941	STUCK THREADS DUE TO INCIDENT REPORTING IN FEDERATION
27781001	Fix for Bug 27781001
27732020	ADMINISTRATION REVOKED USER SHOULD NOT ACCESS APP DOMAIN BY REST OPERATION
27663475	Fix for Bug 27663475
27605692	TECHP: LDAP_SSL_PROTOCOL SETTING REMOVED AFTER UPDATING IDSTORE VIA OAMCONSOLE
27601504	OAUTH - NO CUSTOM ATTRIBUTES IN ACCESS TOKEN
27584074	IMPORTACCESSSTORE FAIL: MISMATCHED NO. OF ENTITIES BEFORE & AFTER TRANSFORMATION
27578580	CUSTOMWAR FILE NEEDS TO INCLUDE THE FORGOT PASSWORD PAGES
27528858	SESSION AUDIT:INCORRECT REQUEST TYPE DISPLAYED FOR GET, UPDATE & DELETE COMMANDS
27506785	INT STG PRIMRY: WEBGATE CONNECTIVITY ISSUES AFTER APPLYING BP13 PATCH
27492241	OAM: DISPLAYWEBGATE11AGENT WLST: DOES NOT DISPLAY LOGOUTURLS
27440104	OAM 12C: OAUTH: CANNOT CHANGE KEYATTRIBUTENAME VALUE
27355457	STRESS:12COAM:NULLPOINTEREXCEPTION IN OAUTH CREATEDOMAIN NEGATIVE STRESS TEST
27338937	DIAG LOG MESSAGES TRACING LOGOUT WORKFLOW
27287517	UPDATING GETOTP.JSP IN OAM-SERVER.EAR TO WORK IN DCC TUNNELLING CASE

Base Bug Number	Description of the problem
27255144	FIX OAMCUSTOMPAGES IN 12C
27203475	OIDC:SPACE CHAR SHOULD BE NOT ALLOWED TO USE FOR RESERVER NAME
27149541	NOTIFICATIONS 'DIAGNOSTICCOOKIECONFIG' AFTER UPGRADING OAM 11.1.2.2 TO 11.1.2.3
27072426	UNABLE TO VIEW ALL IPS IN AUTHORIZATION POLICY IN APPLICATIO DOMAIN OAM CONSOLE
27050584	HOW TO MAKE IDP DN MAPPINGS CASE INSENSITIVE WITH 11.1.2.3 FEDERATION **Note:** To enable Case insensitive feature for DNIDPMapping , run the following wlst command: `putBooleanProperty("/dnidpmapping/ caseinsensitive", "true");`
27028826	TECHPLAT: OAM 12.2.1.3 FAILS TO CONNECT TO LDAPS
26912813	"AGENT TYPE" IS NULL IN OAM ADMIN CONSOLE IF WEB BROWSER LANGUAGE IS JAPANESE
26864424	"ALLOW OAUTH TOKEN" AND "ALLOW SESSION IMPERSONATION" SHOULD BE REMOVED FROM OAM
26844537	EDITWEBGATE11GAGENT UPDATE CAUSES ERRORS WHEN ACCESS WG AGENT FROM CONSOLE
26843227	THERE IS A BROKEN LINK FOR "CREATE X509 AUTHENTICATION MODULE"

Base Bug Number	Description of the problem

26784192	USING IDENTITY CONTEXT IN AUTH PLUGIN OAM
	
	Note:
	
	In order to access ResourceID and AgentAppDomain from authentication context in a custom authn plugin, use:
	
	`authenticationContext.getStringAttribute("ResourceId")` and `authenticationContext.getStringAttribute("AgentAppDomain")`
	Format of the expected parameters:
	
	`ResourceID contains <resourceType>::<HostIdentifier>::<resourceURL>`
	
	`AgentAppDomain contains APP:<AppDomain>| AGENT:<AgentType>:<WebgateID>`
	
	For Example,
	
	ResourceID = HTTP::RREG_HostId11G::/hostid/**::
	
	AgentAppDomain = APP:NewAgent| AGENT:0:TWG_49

26630561	DIAG: NEED DETAILED DEBUG OUTPUT FOR TOTPPLUGIN
26540242	OAM 11.1.2.3 AUTHENTICATION FAILURE CODE NOT AUDITED
26535030	ADD RESILIENCY CHECK FOR POLICY CACHE IN OAM CLUSTERS

Base Bug Number	Description of the problem
25900160	OAM_RES NEEDS TO BE CONFIGURABLE IN PS3 TO BEHAVE LIKE PS2
	Note: The following sample configuration segment is introduced in the oam-config.xml when the WLST command displayAuthZCallBackKey() is executed:

```
Xpath : "/DeployedComponent/
Server/NGAMServer/Profile".

<Setting Name="AuthZCallBack"
Type="htf.map">
<Setting Name="AuthZHashKey"
Type="xsd:string">1E8461DFA32AD746
AF28BAAAA9F327327941C14CAC216DCFA9
AC17985E097A0DD603EC1DF5C6D9F5C904
ED44952A5D5F</Setting>
<Setting
Name="AuthZCallBackEnabled"
Type="xsd:boolean">true</Setting>
</Setting>
```

If `AuthZCallBackEnabled` is set to `false`, then both `oam_res` and `oam_res_hash` are not populated. Only redirection occurs to configured AuthZ Success URL.

If `AuthZCallBackEnabled` is set to `true` then both `oam_res` and `oam_res_hash` are populated with its values after redirection occurs to configured AuthZ Success URL.

Resolved Issues in 12.2.1.3.180414

Base Bug Number	Description of the problem
27605234	OAM12C: ADMIN REST API AUTHNPOLICY IS FAILING WITH REQUEST FAILED

Base Bug Number	Description of the problem
27371324	MAKE PASSWORDMANAGEMENTMODULE AS THE DEFAULT MODULE FOR OAM FRESH INSTALL
	Note: In case of patched environment for BP02, the `PasswordPolicyValidationScheme` will use the original Password policy validation module. Customers who wish to use Multiple Password Policy feature, Forgot Password using OTP and Changing User Status using REST API has to manually change the module that `PasswordPolicyValidationScheme` is using to `PasswordPolicyManagementModule`.
27314613	OIF : IDP INITIATED FLOW WITH USER PROVISIONING PLUG-IN ENABLED DISPLAYS SYSTEM
27206989	ABILITY TO UPDATE CONFIGURATION USING REST
27205555	LOGOUT DONEURL WITH ISALLOWSCHEMERELATIVEURLS SET PERMIT NON-WHITELISTED URL
	Note: To enable/disable scheme relative url , add `isAllowSchemeRelativeURLS` boolean attribute to `oam-config.xml` file, and set the value to true/false respectively.
	Example:

	<pre><Setting Name="EndURLWhiteList"
	Type="htf:map">
	    <Setting
	Name="isAllowSchemeRelativeURLS"
	Type="xsd:boolean">true</Setting>
	    <Setting
	Name="enableWhiteListValidation"
	Type="xsd:boolean">true</Setting>
	    <Setting Name="WhiteListURLs"
	Type="htf:map">
	    </Setting>
	</Setting></pre>

27202829	NOTIFICATION MESSAGES "OAM-CONFIG.XML AS :EXTER" CONSTANTLY LOGGING IN OAM LOGS

Base Bug Number	Description of the problem
27161546	Fix for Bug 27161546
	Refer to technical note Doc ID 2386496.1 available on My Oracle Support. You can access My Oracle Support at https://support.oracle.com.
	Note: By default, the fix for this bug is disabled. The fix can be enabled by adding `globalHMACEnabled` as `true`. If the flag is not present or is present with value `false`, then the fix is disabled.
	Before enabling the fix, it is to be ensured that all webgates are patched with complementary fix (Bug: 27258588, 27355601, and 27568356). For patching webgate, follow webgate patching process.
	Path: `NGAMConfiguration>DeployedComponent> Server>NGAMServer>Profile>oamproxy`
	Caution: If all the webgates are not patched and the flag is enabled, then all those webgates which are not patched will not work.
	Following is the process to introduce/update the flag value:
	• Create a `config.properties` file with the following content:

	`oam.entityStore.schemaUser=[OAM Schema Name]`
	`oam.entityStore.ConnectString=j dbc:oracle:thin:@[Database Host]:[DB Port]:[Service_ID]`
	`oam.entityStore.schemaPassword =[Schema Password]`
	`oam.importExportDirPath=[Direct ory where oam-config.xml will be exported/(imported from)]`
	`oam.frontending=params=host;por t;protocol`

	Note: Put `oam.frontending` line as is for the command to work in above config file.
	• Export the entire `oam-config.xml` using the following command:
	`bash-4.1$ cd [Middleware_Home]` `bash-4.1$ [JDK/JRE_Home]/bin/ java -cp`

Base Bug Number	Description of the problem
| | ```
./idm/oam/server/tools/config-
utility/config-utility.jar:./
oracle_common/modules/
oracle.jdbc/ojdbc8.jar
oracle.security.am.migrate.main
.ConfigCommand
[OAM_Domain_Home] export[Path]/
config.properties
``` <br><br> **Note:** <br> – `config.properties` is the file created in step 1. `oam-config.xml` will be exported to path [oam.importExportDirPath] <br> – Line breaks in above command are only for demonstration purposes. <br> • Now change the value of field `globalHmacEnabled` to `true/false` <br> • Import the updated `oam-config.xml` using the same command used in step:2 , just change `export` to `import`. |
27361854	Fix for bug 27361854 **Note:** This bug is dependent on bug 27161546. Along with this, complementary fix on webgate side is covered by bug 27355601.
27853736	DCC RELOGIN FLOW AFTER IDLE TIME OUT DISPLAY SYSTEM ERROR PAGE **Note:** This bug is dependent on bug 27361854.
27132341	INT STG PRIMARY OAM - UNABLE TO LOGIN TO NEW AGENTS AFTER OCT17 BP
27095174	OPENIDCONNECT SUPPORT FOR OAM SERVER
27084858	PSFE ENHANCEMENT TO RUN FOR BUNDLE PATCH UPDATES
27068410	DISABLE PLAINTEXT OBRAREQ/OBRAR FRONT CHANNEL
26914133	POST DATA PRESERVATION DOES NOT WORK WHEN POST DATA IS LARGER THAN 1200 BYTES
26901175	PASSWORDOLICYREST:: DELETING ALL PASSWORD POLICIES SHOWS INCORRECT MESSAGE
26862217	POLICY SYNC TO MANAGED SERVERS IS VERY SLOW WHEN APPDOMAIN HAS LOT OF RESOURCES

Base Bug Number	Description of the problem
26479576	SAML-PROTECTED APPLICATION USING FRAMES IS BROKEN BY RETURN OF CLICKJACKINGSCRIP
	Note: This fix validates the correct url i.e. the next redirect url against WhiteListURLs in federation flow.
	After applying the patch and before starting OAM nodes. Add the following setting to `oam-config.xml` file under `<Setting Name="EndURLWhiteList" Type="htf:map">` with the REQUEST_URL_KEY that you want to use against WhiteListURLs check.
	`<Setting Name="FedActionUrlKey" Type="xsd:string"><REQUEST_URL_KEY></Setting>` **Example:**

	`<Setting Name="EndURLWhiteList" Type="htf:map">`
	`<Setting Name="FedActionUrlKey" Type="xsd:string">oracle.security. fed.post.actionurl</Setting>`
	`</Setting>`

26286819	STRESS:12C OAM- DEADLOCK DETECTED IN OAM DB DURING STRESS TEST
25867806	ENT INT STG DR-TR - PATCH REQUIRED FOR DELETION OF OSSO AND FEDERATION PARTNERS
25369080	DI BASED ON BUG 23745818 : LOGS TO INDICATE FED DEFAULT AUTHN SCHEME ID
25170276	PARAMETER "EMAILMSGFROMNAME" BEING IGNORED IN OTP E-MAILS
24357957	OAM WHITELIST SHOULD HAVE CONFIG TO ENABLE/DISABLE HOSTID CHECKS
	Note: Enable/Disable the HostId validation mode using WLST command: `oamSetHostIdValidationMode`(default is true).
23185976	VALIDATE WEBGATEID WHEN RUNNING WLST : UPDATEWEBGATETEMPLATETOWEBGATE MAPPING

Resolved Issues in 12.2.1.3.171121

Table 1-10   Resolved Issues in Release 12.2.1.3.171121

Base Bug Number	Description of the Problem
27077697	FORGOT PASSWORD FUCNTIONALITY USING ONETIMEPIN IN OAM
26821988	OAM : IFRAMEBURSTOUT IN BOTH OAMWHITELISTMODE TRUE AND FALSE
26743138	SKIP_AUTHN_RULE_EVAL SHOULD BE ENABLED BY DEFAULT
26732813	SESSION REST GET/SEARCH RESULT DOES NOT CONTAIN THE EXPIRYTIME ATTRIBUTE
26679791	FIX FOR BUG 25898731 IS FAILING IN OAM 11.1.2.3.171017BP 26540179
26672990	IMPERSONATION SESSION IS ALWAYS CREATED WITH LEVEL 2 **Note:** To update the default auth level for impersonation, a new entry `MaxAuthlevel` is introduced in *oam-config.xml* under `ImpersonationConfig`. Example: `<Setting Name="MaxAuthLevel" Type="xsd:string">4</Setting>` Pre-Requisite: Update authentication level of `/oamImpersonationConsent` under IAMSuite domain to match the `MaxAuthLevel`.
26671436	NULL POINTER EXCEPTION IS THROWN WHILE ENABLING SSL FROM OAMCONSOLE
26610754	ER 20773096: ADD ONE NEW WLS CMD FOR WEBGATETEMPLATE REMOVAL
26443261	STEP NUMBER NOT INCREMENTING IN OAM CUSTOM PLUGIN
26429287	ADD WLST FOR SKIP_AUTHN_RULE_EVAL CONFIG PARAMETER
26420974	DETERMINE WHETHER AGENT IS DCC WEBGATE
26375044	AUTHENTICATION FAILING FOR USER-AGENT MATCHING PRE-AUTHN RULE **Note:** This bug has a dependency on Webgate bug 26389702.
26335555	TOTPLUGIN - CAN ACCESS THE APPLICATION WITH AN EXPIRED TOKEN
26226156	OIF: FEDUSERPROVISIONING PLUGIN CREATING ADDITIONAL ENTRIES FOR UID
26199993	NO SOUND/VIBRATE FROM THE PUSH NOTIFICATION ON THE PHONE SIDE

Table 1-10   (Cont.) Resolved Issues in Release 12.2.1.3.171121

Base Bug Number	Description of the Problem
26180201	GLOBAL LOGOUT FAILS AT OAM AS SP WHEN END_URL CONTAINS QUERY PARAMS
26170087	USER GETTING OAM-7 ERROR WHEN ACCESSING SAML (FED) APP INSIDE OF IFRAME (EVEN WHEN WHITELISTED)
26161468	REDIRECT LOGOUT URL WITH WHITE LIST ENABLED PERMIT REDIRECT ON NON LISTED SITE
26147809	IN FORCE PASSWORD ONLY BROWSER LEVEL VALIDATION IS WORKING
26143230	PRE-AUTHN RULE NOT EVALUATED WHEN SWITCHING FROM DCC SCHEMA
26114972	OAM LOGOUT URL NOT BEHAVING AS EXPECTED
25961607	CONFIGUREPOLICYRESPONSES NOT WORKING FOR PASSWORD POLICY DATE STRING AT 11.1.2.3
25709831	CHANGEPASSWORD AFTER PASSWORD EXPIRY:OAM IS NOT RETURNING THE REASON/ERROR CODE
25534524	LOOP ON SYSTEMERROR WHEN USER SITS FOR OVER 15 MINUTES ON BOOKMARKURL LOGIN PAGE
25485089	DIAG: OPENID ASSOCIATION FAILED FOR RESPONSEHANDLEREXCEPTION
25315550	ADVANCED RULES NOT WORKING IN CLONED ENVIRONMENT AFTER BEING IMPORTED

24817439	SAML ASSERTION HAS INCORRECT DATA FORMAT FOR NAMEID-FORMAT:ENTITY
	
	Note: This feature is added to either disable sending Format attribute on Issuer or set it to Unspecified or entity value. This can be set at partner, profile or global level.
	
	After applying the fix, following WLST command needs to be executed:
	
	`domainRuntime()`
	
	`updatePartnerProperty("<IDP-partner-name>","idp",`
	`"sendsamlissuerformat", "false",`
	`"boolean")`
	
	Example: updatePartnerProperty("lcr01103-idp", "idp", "sendsamlissuerformat", "false", "boolean")

Table 1-10   (Cont.) Resolved Issues in Release 12.2.1.3.171121

Base Bug Number	Description of the Problem
24746284	IDENTITY CONTEXT CLARIFICATION ON PUBLISHED ATTRIBUTES FORMAT
	Note: To use the new format for custom attributes, before starting the OAM Managed Server, set the system property `oracle.oam.saml.assertion.customattr format=SAML2.0` using the following command, `export JAVA_OPTIONS="-Doracle.oam.saml.assertion.customatt rformat=SAML2.0".`
22494562	OAM FEDSTS-11013 ERROR: ORA-00001: UNIQUE CONSTRAINT VIOLATED

Known Issues and Workarounds

Known issues and their workarounds in Oracle Access Management Release 12.2.1.3 are described in the Oracle Access Management chapter of the *Release Notes for Oracle Identity Management* document. You can access the Release Notes document in the Oracle Identity Management Documentation library at the following URL:

https://docs.oracle.com/middleware/12213/idmsuite/IDMRN/toc.htm

> ✏️ **Note:**
>
> Some known issues listed in the Release Notes for Oracle Identity Management may have been resolved by this Bundle Patch (Oracle Access Management 12.2.1.3.0). Compare the issues listed in Resolved Issues of this document when reviewing the *Release Notes for Oracle Identity Management*.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
OAM BUNDLE PATCH 12.2.1.3.210915	32824147	33377719	If the username contains backslash (\\), for example `'doe\john'` then the authentication is successful and the protected resource is accessible. However, the following error is logged in the OAM Server logs: `oracle.igf.ids.EntityNotFoundException`
OAM BUNDLE PATCH 12.2.1.3.210701	32625905	33074398	When using the adaptive authentication module to send push notifications to iOS devices, the mobile device does not play the notification sound when the push notification arrives.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
OAM BUNDLE PATCH 12.2.1.3.200629	31338274	2670747.1	After upgrade from 11.1.2.3.0 to 12.2.1.3.0, and applying the OAM 12.2.1.3.181213 BP configured with Oracle Database version 19.x.x, Admin Server startup fails with the following error: `Internal Exception: java.sql.SQLRecoverableException: IO Error: Broken pipe Error Code: 17002 Call: SELECT FILE_CONTENT FROM OAM_FILE_ARTIFACTS WHERE (ID = ?) FOR UPDATE` For details and workaround, see `Doc ID 2670747.1` at https://support.oracle.com

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
OAM BUNDLE PATCH 12.2.1.3.0 (ID:191201.0123.S)	N/A	2622132.1	When using a `failure_url` in one of the following scenarios, it causes an OAM system error instead of being redirected to the expected or defined failure URL: • Using the OAM impersonation feature and calling the following URL that includes a `failure_url` parameter: `http://<OAMHOST>:<OAMPORT>/oam/server/impersonate/start?userid=<USERNAME>&success_url=<SUCCESS_URL>&failure_url=<FAILURE_URL>` • Using a federation flow for CUSTOM nameid format that includes any failure URL.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
12.2.1.3.190609	N/A	29940526	When you create the identity provider (IdP) or Service Provider (SP) partners using the Oracle Access Management Console, the following error message appears: `"An internal error occurred while creating Identity Provider Partner. Check the logs for additional details."` There is no impact to functionality, and no user action is needed.
12.2.1.3.190609	N/A	N/A	WebGate 12*c* is using the underscore (_) for host and port separator in Authentication cookie names. For example, the OAMAuthnCookie name format `OAMAuthnCookie_example.com:443` is now replaced as `OAMAuthnCookie_example.com_443`. This leads to SSO failure between the Detached Credential Collector (DCC) and DCC Tunneled resources as the server continues to use the older cookie name format. To resolve this issue, add `UniqueCookieNames=legacy` to the to the User-defined parameters of the DCC WebGate profile. This will allow Webgate to use older cookie name format.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
12.2.1.3.180904	MOS Note ID: 2460270.1	28277233	There is a policy corruption issue which occurs when there are multiple webgates with multiple resources. The end user will not be allowed to access the application. Customers encountering this issue should request a one-off patch.
12.2.1.3.180706	N/A	N/A	The only supported response_type for /authorize endpoint to OIDC Server is code i.e.response_type=code .
12.2.1.3.180414	27068410	27606513	`disable10gPlainTextReqRes`parameter is case sensitive Workaround is to use `disable10gPlainTextReqRes` parameter as it is. Do not change the case.
	27068410	27606466	The functionality does not work when Agent and Preferred Host are different for the registered 10g Webgate Agent Profiles. Workaround is that the Agent Name and Preferred Host has to be same for the registered 10*g* Webgate Agent Profiles.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
	27068410	27626433	Functionality does not work when bulk updates are done for updating the `userdefinedparam` of 10*g* agent profiles. Workaround is to update the `userdefinedparam` of all the 10*g* agent profiles manually using the oamconsole.
	27582324		POST data restoration will not work with `ChallengeRedirect Method=GET` Workaround is to set, `ChallengeRedirect Method=post` in the Authentication scheme.
12.2.1.3.171121	27292760		There are cases when `AdaptiveAuthentic ationPlugin` does not contain the required fields to enable the OTP. The Workaround is to add the required fields to update the properties in `oam-config.xml` file by adding them to the `ConfigParams` section of the `OAMMFAOTP` definition.