Oracle® Fusion Middleware

Oracle Access Management Bundle Patch Readme

Bundle Patch 12*c* (12.2.1.3.190609) Generic for all Server Platforms

F18791-01

July 2019

Oracle Access Management Bundle Patch Readme

This document describes Bundle Patch 12c Release (12.2.1.3.190609) for Oracle Access Management.

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:

- Understanding Bundle Patches
- Bundle Patch Requirements
- Applying the Bundle Patch
- Removing the Bundle Patch
- Resolved Issues
- Known Issues and Workarounds

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.

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 (version 13.9.2.0.0+ 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 -help` to check if your Opatch version is earlier than 13.9.2.0.0. If so, download the latest 13.9.2.0.0 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 p29887467_122130_Generic.zip
2. Unzip the patch zip file into the PATCH_TOP.

```
$ unzip -d PATCH_TOP p29887467_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 p29887467_122130_Generic.zip
```

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

   ```
   $ cd PATCH_TOP/29887467
   ```

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.

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/29887467`
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 29887467
   ```

   > **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 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 12.2.1.3.190609

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

Table 1-1 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

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

Base Bug Number	Description of the Problem
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>`
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
29240849	NEED TO LOG ADDITIONAL AUTHENTICATION FAILURE FOR AUDIT LOG FROM CUSTOM PLUGIN

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

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

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>"`

Table 1-1 (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`.
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 1-1 (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 1-1 (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_JNDILDAPREADTIMEOUT="15000"` • `export ORACLE_OAM_JNDILDAPREADTIMEOUT`
27946582	WNA POST FALLBACK IS FAILING AFTER APPLYING BP13
27708019	OAM11.1.2.3 : FEDERATION: LOGOUT SAMLRESPONSE DOES NOT INCLUDE RELAYSTATE.

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

Base Bug Number	Description of the Problem
27441865	CLIENTSSLKEYSTOREPWD, CLIENTSSLTRUST-STOREPWD 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="clientsslkeystorepwd", user="UniqueUserNameCredential", password="mypassword", desc="identity keystore pwd")`
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/)

- `<SettingName="PolicyCacheComponent" Type="htf:map">.....</Setting>`

Base Bug Number	Description of the problem
	• <Setting Name="PolicyCache-Management-tAPI" Type="htf:map"> ..... </Setting>
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="," ,respon-
```

Base Bug Number	Description of the problem
	seEscape-Char="\\")
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 `displayFedCustomAuditE-`

Base Bug Number	Description of the problem
	vents() to configure 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 PRE-SET **Note:** • This bug has a dependency on OPSS October Bundle Patch. Please apply OPSS Bundle Patch 12.2.1.3.181016:28172453along 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 REMOVEWEB-GATETEMPLATEPARAMS WHITH NON-EX-ISTING 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 WEB-GATE
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 KEY-ATTRIBUTENAME 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
27255144	FIX OAMCUSTOMPAGES IN 12C

Base Bug Number	Description of the problem
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">1E8461DFA32AD746AF28BAAAA9F327327941C14CAC216DCFA9AC17985E097A0DD603EC1DF5C6D9F5C904ED44952A5D5F</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:
	`<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>`

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>oam-proxy`
	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=jdbc:oracle:thin:@[Database Host]:[DB Port]:[Service_ID]`
	`oam.entityStore.schemaPassword=[Schema Password]`
	`oam.importExportDirPath=[Directory where oam-config.xml will be exported/(imported from)]`
	`oam.frontending=params=host;port;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/`

Base Bug Number	Description of the problem
	`java -cp ./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` **Note:** – `config.properties` is the file created in step 1. `oam-config.xml` will be exported to path [oam.importExportDirPath] – Line breaks in above command are only for demonstration purposes. • Now change the value of field `globalHmacEnabled` to `true/false` • 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 : UPDATEWEBGATETEMPLATETOWEBGATEMAPPING

Resolved Issues in 12.2.1.3.171121

Table 1-2 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 USERAGENT 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 1-2 (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 1-2 (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.customattrformat=SAML2.0` using the following command, `export JAVA_OPTIONS="-Doracle.oam.saml.assertion.customattrformat=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
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.
	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.

Bundle Patch Number	Base Bug Number/Doc ID	Bug Number/Doc ID	Description of the Problem
	27582324		POST data restoration will not work with `ChallengeRedirectMethod=GET` Workaround is to set, `ChallengeRedirectMethod=post` in the Authentication scheme.
12.2.1.3.171121	27292760		There are cases when `AdaptiveAuthenticationPlugin` 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.

Oracle® Fusion Middleware Oracle Access Management Bundle Patch Readme, Bundle Patch 12*c* (12.2.1.3.190609) Generic for all Server Platforms
F18791-01

Copyright © 2019, 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.