**Oracle® Fusion Middleware**

Oracle Access Management Bundle Patch Readme

OAM Bundle Patch 14.1.2.1.250916 Generic for all Server Platforms

G30317-02

October 2025

# Oracle Access Management Bundle Patch Readme

This document describes OAM Bundle Patch 14.1.2.1.250916.

This document requires a base installation of Oracle Access Management 14c (14.1.2.1.0) and contains the following sections:



## New Features and Enhancements in OAM Bundle Patch 14.1.2.1.250916

Oracle Access Management 14.1.2.1.250916 BP includes the following new features and enhancements:

- **Ability to Pass MFA Claim in SAML Assertion When OPENIDCONNECT or SAML (AMR Claim) is Used** (ER 37358122)
  This enhancement allows administrators to modify the "amr" and "acr" fields in an OIDC token while using the OpenIDConnect plugin. It can also be used to set multi-factor bypass assertion in the resulting SAML assertion message with federated systems using SAML2.0. This helps bypass second factor multi-factor authentication. Specifically, this can be achieved using the following:
  - Using OpenIdConnect Plugin:

        * If the federation is implemented via OpenIdConnect plugin, then edit the challenge parameters of the configured authentication scheme in OAM (acting as IdP) to "AMR=mfa".
        * The pipe character "|" can be used if multiple values are required.
          For example: `"AMR=mfa|mca|fido"`
        * Set "ACR=<value>" in the challenge parameters box of the configured authentication scheme.
          For example: `"ACR=urn:oracle:loa:1fa:wia"`
        * Result: "amr" and "acr" claims in the OIDC token contain the configured values.
    - Using SAML2.0 Federation:
        * If the federation is implemented via SAML2.0, then add "AMR=mfa" in the challenge parameters box of the configured authentication scheme in OAM (acting as a Service Provider).
        * If multiple values are present in the AMR string, it will check if the string contains "mfa".
          For example: `"AMR=pwd|mfa|cert"`
        * Result: The resulting assertion message will contain "http://schemas.microsoft.com/claims/multipleauthn" as AuthnContextClassRef inside AuthnStatement, which will bypass the second factor MFA.
    - Using TAP Token:
        * For bypassing the second factor MFA in federated systems authenticated via a TAP token, the "amr" value can be set to "AMR_STR" and the "acr" value can be set to "ACR_STR" in the Token Map.
        * Result: TAP Token will contain the configured values of "amr" and "acr".

      > **Note**
      >
      > For more information, refer to Doc ID 3107754.1 at https://support.oracle.com.

- **Ability To Use Custom Code To Return Response Values** (ER 36846382)
  This allows administrators to write code that generates the required response value using the context provided by OAM. For more information, see Setting Response Values Programmatically.

## Understanding Bundle Patches

Describes Bundle Patches and explains the differences between Stack Patch Bundles, Bundle Patches, interim patches and Patch Sets.

- Stack Patch Bundle
- Bundle Patch
- Interim Patch

- Patch Set

## Stack Patch Bundle

Stack Patch Bundle deploys the IDM product and dependent FMW patches using a tool. For more information about these patches, see `Quarterly Stack Patch Bundles (Doc ID 2657920.2)` at https://support.oracle.com.

## Bundle Patch

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

## Interim Patch

In contrast to a Bundle Patch, an interim patch addresses only one issue for a single component. Although each interim patch is an official Oracle patch, it is not a complete product distribution and does not include packages for every component. An interim patch includes only the libraries and files that have been rebuilt to implement a specific fix for a specific component.

You may also know an interim patch as: security one-off, exception release, x-fix, PSE, MLR, or hotfix.

## 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 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 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 `Stack Patch Bundle for Oracle Identity Management Products (Doc ID 2657920.2)` 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.
3. It is mandatory to apply one-off patch 38181053.

## Applying the Bundle Patch

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

- Using the Oracle Patch Mechanism (OPatch)
- Applying the OAM Bundle Patch
- Recovering From a Failed Bundle Patch Application

> **Note**
>
> - You must install the following mandatory patches:
>   - OPSS: 36316422
>   - OWSM: 38073767
>   - OINAV: 38009014
>   - WLS Patch:38412437
>   - libovd: 36649916
>   - EM: 36946553
>   - ADF: 38348152
>   - Coherence: 38409281
>   - FMW Thirdparty Bundle: 38405729
> - From March 2024, the Oracle Access Manager (OAM) components using SIMPLE-mode certificates for communication will not work, resulting in an outage in the OAM environment, unless preventive measures are taken. For more information, see *March 2024 Expiration Of The Oracle Access Manager (OAM) Out Of The Box Certificates (Doc ID 2949379.1)* at https://support.oracle.com.

## 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 variable, 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 the Bundle Patch application. The subset patch is automatically rolled

back before the 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 need to be running. The Machine Name & Listen Address can be blank on a default install.

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

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

- Log in to My Oracle Support: https://support.oracle.com/
- Download the required OPatch version.
- Use `opatch version` to check if your OPatch version is the latest. If it is an earlier version of OPatch, download the latest version.
- Confirm if the required executables opatch and unzip are available in your system by running the following commands:

  Run *`which opatch`* - to get the path of OPatch

  Run *`which unzip`* - to get the path of unzip

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

  ```
  opatch lsinventory
  ```

  Windows 64-bit: `opatch lsinventory -jdk c:\jdk21`

  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 the information and steps found 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 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 p38434987_141210_Generic.zip
2. Unzip the patch zip file into the `PATCH_TOP`.

   ```
   $ unzip -d PATCH_TOP p38434987_141210_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 p38434987_141210_Generic.zip
   ```

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

   ```
   $ cd PATCH_TOP/38434987
   ```

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`.
- 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\jdk21`

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

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

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

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

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

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

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

   ```
   connect('weblogic','XXXX','t3<a target="_blank" href="://
   localhost:7001'">://localhost:7001'</a>)
   domainRuntime()
   setMultiDataCenterWrite(WriteEnabledFlag="true")
   ```

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

   ```
   connect('weblogic','XXXX','t3<a target="_blank" href="://
   localhost:7001'">://localhost:7001'</a>)
   domainRuntime()
   setMultiDataCenterWrite(WriteEnabledFlag="false")
   ```

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

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

## Recovering From a Failed Bundle Patch Application

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

To recover from a failed Bundle Patch application:

1. Confirm that there are no configuration issues with your patch application.
2. Confirm that you can start the AdminServer successfully.
3. Shut down the AdminServer and rollback the patch as described in Removing the Bundle Patch then apply the Bundle Patch 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\p38434987_141210_Generic\384349
> 87
> >c:\Oracle\oam12214\OPatch\opatch rollback -id 38434987
> 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 the steps in Applying the OAM Bundle Patch to set the 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/38434987`
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 rollback the patch. For example:

   ```
   opatch rollback -id 38434987
   ```

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 Bundle Patch provides the fixes described in the below section:

- Resolved Issues in OAM Bundle Patch 14.1.2.1.250916
- Resolved Issues in OAM Bundle Patch 14.1.2.1.250701
- Resolved Issues in OAM Bundle Patch 14.1.2.1.250318

## Resolved Issues in OAM Bundle Patch 14.1.2.1.250916

Applying this Bundle Patch resolves the issues listed in the following table:

**Table 1-1 Resolved Issues in OAM Bundle Patch 14.1.2.1.250916**

| Bug | Description |
|---|---|
| 37639134 | DYNAMIC ATTRIBUTES ARE NOT RETURNED CORRECTLY AFTER USING REFRESH TOKEN |
| 37358122 | ER- Ability to Pass MFA Claim in SAML Assertion When OPENIDCONNECT or SAML (AMR Claim) is Used<br>For more information see New Features and Enhancements in OAM Bundle Patch 14.1.2.1.250916 |
| 36690163 | OAM (SP) ISSUE WHEN USING SAML FED IDP WITH MIX OF ARTIFACT BINDING HTTP & HTTPS (SSL-2WAY) |
| 38059257 | EXPIRY_TIME COLUMN IS NOT CREATED AFTER APPLYING OCTOBER BP |
| 38160707 | OAM 12C LOG FILES FILLED WITH WARNING MESSAGES |

**Table 1-1 (Cont.) Resolved Issues in OAM Bundle Patch 14.1.2.1.250916**

| Bug | Description |
|---|---|
| 37965826 | KEY_OPS ATTRIBUTE ON OIDC KEYPAIR<br><br>**Note**<br>Introduced OAuth domain level custom attribute "enablejwkkeyuse" to make this fix work.<br>Example:<br>`curl -X PUT -H 'Content-Type: application/json' --user <ADMIN_USER:ADMIN_PASSWORD> http://<OAM_ADMIN_HOST>:<ADMIN_PORT>/oam/services/rest/ssa/api/v1/oauthpolicyadmin/oauthidentitydomain?name=<OAUTH_DOMAIN> -d '{"customAttrs":"{\"enablejwkkeyuse\":\"true\"}"}'` |
| 26100328 | HELP INCORRECT FOR COMMAND SETMULTIDATACENTERWRITE |
| 29534291 | FEDERATION : PARTNER INFO API RETURNS EXPIRED CERTIFICATE WHEN MULTIPLE EXIST |
| 27574109 | NOT ABLE TO LOAD METADATA AUTOMATICALLY TO 12C |
| 36103295 | Fix for Bug 36103295 |
| 38107753 | OAM CONSOLE BROKEN LINKS TO APPLICATION SECURITY AND CONFIGURATION DASHBOARDS |
| 38054681 | OAUTH : NOT ABLE TO FORCERELOGINWITHRTREUSE TO FALSE |
| 38065860 | WRONG ALGORITHM DISPLAYED ON /OAUTH2/REST/SECURITY |
| 37923669 | Fix for Bug 37923669 |
| 36846382 | SET RESPONSE HEADERS TO VALUES OBTAINED PROGRAMMATICALLY |

## Resolved Issues in OAM Bundle Patch 14.1.2.1.250701

Applying this Bundle Patch resolves the issues listed in the following table:

**Table 1-2 Resolved Issues in OAM Bundle Patch 14.1.2.1.250701**

| Base Bug Number | Description of the Problem |
|---|---|
| 38032967 | ACCESS TOKENS ARE NOT GENERATED IF THE SESSION CLIENT IP AND THE REQUEST CLIENT IP DIFFER |
| 37766822 | OAMCONSOLE NOT USING ADMIN PORTS |

**Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 14.1.2.1.250701**

| Base Bug Number | Description of the Problem |
|---|---|
| 37382215 | HELP LINK IN ADMIN CONSOLE IS POINTING TO 12.2.1.3 |
| 37954115 | OAM RETURNS USERNAME AS UUID INSTEAD OF MAIL |
| 37287932 | ASDK ERROR - EXCEEDING SESSION LIMIT NUMBER |
| 37912418 | INCORRECT AUDIENCE ON TOKEN_EXCHANGE GRANT TYPE |
| 35929678 | HARD CODED INDEX HINT CAUSING SQL PERFORMANCE REGRESSION FOR BUGFIX 35591710 |
| 37321460 | PASSWORD RULES ARE NOT DISPLAYING IN DUTCH IN PASSWORD RESET FLOW |
| 37208431 | FORGOTPASSWORD WITH OTP DOESN'T REDIRECT TO LOGIN IF SERVERREQUESTCACHETYPE=FORM |
| 37383063 | ATTRIBUTE LATESTOTPDATASFAPIN WHICH IS NOT ALLOWED BY ANY OF THE OBJECTCLASSES |
| 37559207 | SCRIPT-SRC & STYLE-SRC CSP DIRECTIVES BREAK THE DEFAULT OAM WEBPAGES |
| 37815193 | OAM IDP FOR SAML SOAP CALL RECEIVE "UNKNOWN ASSERTION ARTIFACTS" |
| 35560291 | FEDERATION PROXY NOT FORWARDING THE AUTHENTICATION CONTEXT |
| 37749984 | REMOTE IP IS NOT VISIBLE FROM IAU_REMOTEIP OF IAU_BASE TABLE FOR OAUTH AUTHORIZATION |
| 37729703 | FIX MEMORY LEAKS CAUSED BY THE USE OF GRAAL LIBRARY |
| 37339447 | 400 BAD REQUEST ERROR IS RETURNED BY NGINX INGRESS CONTROLLER |

**Note**

Set the following system property in the `setDomainEnv.sh` to enable the feature

```
-
Doracle.oam.oauth.
redirecturi.decode
=true
```

**Table 1-2 (Cont.) Resolved Issues in OAM Bundle Patch 14.1.2.1.250701**

| Base Bug Number | Description of the Problem |
|---|---|
| 37762292 | ER - OAM : PROCEDURE FOR CHANGING (NOT RESETTING) THE .OAMKEYSTORE PASS<br><br>**Note**<br>`resetOAMKeystorePassword` WLST command enhanced to provide password for `.oamkeystore keystore`.<br>For example:<br>resetOAMKeystorePassword(propsFile='/refresh/home/amit.properties', domainHome='/refresh/home/Oracle/Middleware_IAM/Oracle_Home/user_projects/domains/oam_domain', keyStorePswd='hsadh$23jdsGeeksportal20') |
| 37634307 | OAM : ADD ADDITIONAL LOG MESSAGES TO TRACK LOGOUT FLOW |
| 37917993 | OMA MANAGEMENT SERVICE API |
| 37389548 | ACCESS TOKEN FOR MULTIPLE SCOPE ID IS NOT WORKING IN OCT BP 2024 |
| 37790226 | ACCESS TOKEN AUDIENCE MISSING CLIENT ID IN REFRESH TOKEN FLOW |

## Resolved Issues in OAM Bundle Patch 14.1.2.1.250318

Applying this Bundle Patch resolves the issues listed in the following table:

**Table 1-3 Resolved Issues in OAM Bundle Patch 14.1.2.1.250318**

| Base Bug Number | Description of the Problem |
|---|---|
| 37594407 | FMW 141210: OAM STOP MANAGED SERVER THROWS EXCEPTION |

## Related Documents

For more information, see the following resources:

- Administering Oracle Access Management

  This guide provides information on administration and configuration tasks using Oracle Access Management.

- Developing Applications with Oracle Access Management for All Platforms

  This guide explains how to write custom applications and plug-ins to programmatically extend access management functionality using the SDKs and APIs provided with Oracle Access Management.

---

Oracle Fusion Middleware Oracle Access Management Bundle Patch Readme, OAM Bundle Patch 14.1.2.1.250916 Generic for all Server Platforms
G30317-02