Oracle® Fusion Middleware

Oracle Access Management Bundle Patch Readme

OAM Bundle Patch 12.2.1.4.250428 Generic for all Server Platforms

G29738-01

April 2025

Oracle Access Management Bundle Patch Readme

This document describes OAM Bundle Patch 12.2.1.4.250428.

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.250428

Oracle Access Management 12.2.1.4.250428 BP includes the following new features and enhancements:

- **Ability To Use Custom Code To Return Response Values**

  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.

- **Support for WS_FEDERATION active profile for Oracle Universal Authenticator**

  OAM now supports the WS-Federation active profile for Oracle Universal Authenticator, enabling Microsoft Entra ID–joined Windows devices to authenticate via federation when OAM is configured as an external IDP. Configuration is managed through the oam-config.xml file under `/DeployedComponent/Server/NGAMServer/Profile/STS/wstrustactiveglobal`. Administrators must add a key_id entry named wstrust_signing using a new or existing signing key. Once enabled, the following two REST endpoints for the active profile become available:

  - `/fed/oamwsfed/services/trust/mex`
  - `/fed/oamwsfed/services/trust/13/usernamemixed`

- **Support for Configurable Issuer URL and Immutable Attribute Mapping in WS-Federation Active Profile**

  Support has been added to configure a custom issuer URL in cases where the default value, derived from the OAM load balancer configuration, does not match the value expected by the Service Provider (SP). The immutable attribute is now determined based on the uidAttribute specified in the global configuration. Administrators can define the ISSUER_URI by adding the following entry under `/DeployedComponent/Server/NGAMServer/Profile/STS/wstrustactiveglobal`:

  ```
  <Setting Name="providerid" Type="xsd:string">http://
  idminterop.com/oam/fed</Setting>
  ```

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.241009

Oracle Access Management 12.2.1.4.241009 BP includes the following new features and enhancements:

- **Setting the GCM API Key**

Google is deprecating legacy FCM APIs and migrating to HTTP v1 APIs. For all new configurations, it is recommended to use HTTP v1 APIs. For the steps to migrate to HTTP v1 APIs, see Migrating to service account JSON for Android Push Notifications.

- **Automating SAML Certificate or Key or Metadata Rotation**

  You can schedule the retrieval of new partner certificates and metadata via a REST endpoint and seamlessly rotate the updated credentials across all dependent systems and applications without any downtime. For more details, see Automating SAML Certificate or Key or Metadata Rotation.

- **Ability to Load the Fusion Page in Visual Builder (VB)**

  In the Chrome browser, some OAM cookies were blocking the Fusion page from loading in the Visual Builder (VB) after the third-party cookies were deprecated. With this release, Cookies Having Independent Partitioned State (CHIPS) support is added for OAM/Webgate cookies to overcome this issue. For more details, see OAM Cookies Block the Fusion Page from Loading in VB after the 3rd Party Cookies are Deprecated.

- **Ability to Retrieve an ID Token Through an Authorization Code**

  You can retrieve both access and ID tokens when using the refresh token in the authorization code. For more details, see Getting IDtoken via a Refresh Token Request.

- **Best Practices for Oracle Access Manager (OAM) OAuth Security**

  Added best practices for OAM OAuth security that highlight the possible threats and strategies to mitigate those risks. For more details, see Best Practices for Oracle Access Manager (OAM) OAuth Security.

- **OAA Error Handling Plugins**

  Added new plugins to support MFA on the User Preferences page. For more details, see OAA Error Handling Plugins.

- **Ability to Add Partner Signing and Encryption Keys**

  A new **Key Configuration** section was added to the OAM Console allowing you to select the partners signing and encryption keys when creating a new Identity Provider (IdP) or Service Provider (SP). For more details, see Use Oracle Access Manager to sign on to Oracle Private Cloud Appliance.

- **Ability to Configure Reuse Detection for Refresh Tokens**

  Added a new property to detect the reuse of the Refresh Tokens. For more details, see Configuring reuse detection for Refresh Tokens.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.240701

Oracle Access Management 12.2.1.4.240701 BP includes the following new features and enhancements:

- **Connecting with Messaging Server**

If you configured push notifications for Android then you should migrate to HTTP v1 API's by following the steps mentioned in Migrating to service account json for Android Push Notification.

- **Enhanced OAM 12c OAuth to Support RS512 in Addition to RS256 (Default) as the Crypto Algorithm for Signing the OAuth Token**
  - Introduced an OAuth system property (`-DoauthRS512Enabled=true`) to enforce `RS512` crypto algorithm when enabled across all OAuth Identity Domains (Default - `RS256`). Add the system property to `setDomainEnv.sh` to enable this feature.
  - Introduced an OAuth custom attribute (`oauthRS512Enabled=true`) to enforce `RS512` crypto algorithm when enabled on specific OAuth Identity Domains (Default - `RS256`).

> **Note:**
>
> When both are set the system property overrides the OAuth Identity Domain custom attribute in enforcing the `RS512` crypto algorithm.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.240328

Oracle Access Management 12.2.1.4.240328 BP includes the following new features and enhancements:

- **User Password Change Validation**

  Setting the `userPasswordChangeCheckEnabled=true` property in `oam-config.xml` validates the tokens generated before the user password update. If the user updates or changes the password after retrieving the access tokens then those access tokens generated before the password update will be invalid. The user will need to regenerate the access tokens after the password is updated. For details, see Enabling User Password Change Validation.

> **Note:**
>
> Perform a GET operation on the `/DeployedComponent/Server/NGAMServer/Profile/ssoengine/OAuthConfig` endpoint and a PUT operation on the same endpoint to enable User Password Change Validation feature. It ensures that the configuration that has already been applied continues to be effective.

- **Ability to Customize Issuer Discovery Identifier and Iss Token Claim**

  With the implementation of this enhancement, you can mask or omit the port from the issuer and customize the path component in the OpenID configurations. For details, see Custom Issuer Support.

> **Note:**
>
> Perform a GET operation on the `/DeployedComponent/Server/NGAMServer/Profile/ssoengine/OAuthConfig` endpoint and a PUT operation on the same endpoint to enable Custom Issuer Support feature. It ensures that the configuration that has already been applied continues to be effective.

- **Ability to Change Default Consent Acknowledgment Expiry Time**

  A new custom attribute `consentAcknowledgeExpiryTimeInSeconds` allows you to change the default expiry time to acknowledge the consent approval. For details, see Changing Default Consent Acknowledgment Expiry Time.

- **Ability to Set the Expiry Time for ID_TOKEN**

  You can set a token validity/expiry time for ID_TOKEN instead of using the validity/expiry time in the ACCESS_TOKEN settings. For details, see Creating an Identity Domain.

- **Client Secret Expiration and Rotation**

  By using the custom attribute `oldSecretRetentionTimeInDays`, you can configure the time for which the old client secret will continue to work. This custom attribute can be defined both at the domain-level and at the client-level. However, the value defined at the client-level takes precedence. For details, see Creating an Identity Domain.

- **Added New Field to View API Key**

  With this release a new field **API Key** is added in the partner details screen. This field allows administrators to share the key details with the relevant partners for secure updates. For details, see Configuring the Signing and Encryption Key.

- **Ability to Check Authentication Context When OAM is Acting as a Service Provider (SP)**

  If OAM is acting as a SP, it identifies the Authentication Context of any external SAML Identity Provider (IdP) and proceeds with the SAML authentication based on the `authnassurancelevel` property. For details, see Checking Authentication Context when OAM is acting as SP.

- **Ability to Mask SAML Response Attributes in OAM Log Messages**

  With this release, Oracle Access Management masks SAML Response attributes in OAM log messages. For details, see Masking SAML Attributes in Log Records.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.240109

Oracle Access Management 12.2.1.4.240109 BP includes the following new features and enhancements:

- **Propagating an Error Code from OAA Application to the OAM Login Page**

This enhancement propagates an error code from Oracle Advanced Authentication (OAA) application to OAM login page. The login page can be customized to show the error message propagated from OAA.

The following error codes are supported:

- **Error code**: OAA-00001

  Reason: User Registration was incomplete.

  Cause: No factors registered.

- **Error code**: OAA-00002

  Reason: User did not have any usable factors.

  Cause: Maxed out of allowed authentication attempts. Matching factor(s) are disabled. No required factor(s) available for matching Policy.

- **Error code**: OAA-00003

  Reason: User authentication failure.

  Cause: User did not submit valid authentication data.

- **Error code**: OAA-00004

  Reason: System temporarily unavailable.

  Cause: Unexpected failure in Service during login. For example, Failure to send a challenge (Push, Email, SMS), Database outage.

- **Enhancing OAM Session Management Endpoints**
  Introduced a mechanism to authorize OAM endpoints using TAP Tokens.
- **Added Null Checks for Programmatic Authn REST Interfaces**
  The following fixes are made as a part of this enhancement:
  - Resolved the Null Pointer Exception that occurs when No Auth is selected as the authentication method.
  - In the session validation API, Null Pointer throws an exception when a random string is supplied as an `OAM_RM` token.
- **Added `PublicClientRefreshTokenEnabled` Client Custom Attribute to Obtain a Refresh Token with a Public Client**
  By default it is not possible to obtain a refresh token with a public client. The `PublicClientRefreshTokenEnabled` client custom attribute allows you to change this behavior. To enable the feature set the attribute value to true. For example, create the `oauth` public client with the following command:

  ```
  curl -X POST http://<AdminServerHost:Port>/oam/services/
  rest/ssa/api/v1/oauthpolicyadmin/client -H 'Authorization:Basic
  d2VibG9naWM6d2VsY29tZTE=' -H 'Content-Type: application/json' -d
  '{"id":"PublicClientId","name":"PublicClient","scopes":
  ["ResServer1.scope1"],"clientType":"PUBLIC_CLIENT","secret":"welcome
  1","idDomain":"TestDomain1","description":"Client
  Description","grantTypes":
  ["PASSWORD","CLIENT_CREDENTIALS","JWT_BEARER","REFRESH_TOKEN","AUTHO
  RIZATION_CODE"],"defaultScope":"ResourceServerOud1.scope1","redirect
  URIs":[{"url":http://localhost:8080/Sample.jsp,"isHttps":true}],
  ```

```
"attributes":
[{"attrName":"PublicClientRefreshTokenEnabled","attrValue":"true","a
ttrType":"static"}]}'
```

- **Added `GrantTypeRefreshTokenEnabled` Client Custom Attribute to Return a Refresh Token Along with a New Access Token**
  By default, when the grant type is `refresh_token`, only a new access token is returned. The `GrantTypeRefreshTokenEnabled` client custom attribute allows you to have a refresh token returned as well. To enable the feature set the attribute value to true. For example, create the `oauth` confidential client with the following command:

  ```
  curl -X POST http://<AdminServerHost:Port>/oam/services/
  rest/ssa/api/v1/oauthpolicyadmin/client -H 'Authorization:Basic
  d2VibG9naWM6d2VsY29tZTE=' -H 'Content-Type: application/json' -d
  '{"id":"TestClientId","name":"TestClient","scopes":
  ["ResServer1.scope1"],"clientType":"CONFIDENTIAL_CLIENT","secret":"w
  elcome1","idDomain":"TestDomain1","description":"Client
  Description","grantTypes":
  ["PASSWORD","CLIENT_CREDENTIALS","JWT_BEARER","REFRESH_TOKEN","AUTHO
  RIZATION_CODE"],"defaultScope":"ResServer1.scope1","redirectURIs":
  [{"url":http://localhost:8080/Sample.jsp,"isHttps":true}],
  "attributes":
  [{"attrName":"GrantTypeRefreshTokenEnabled","attrValue":"true","attr
  Type":"static"}]}'
  ```

  > **Note:**
  >
  > To revoke the old `refresh_token` while invoking the `refresh_token` grant type set the system property `-Doauth.auto.revoke.enabled=true`. The default value of this system property is false.

- **Support for `Response_mode` in the Authorization Code Grant Flow**
  This enhancement allows 3-legged OAM OAuth 2.0 workflow API (`/oauth2/rest/authorize`) to respond in different modes like fragment , query or `form_post` by specifying `response_mode` as a query parameter.
- **Support for 3-legged OAuth 2.0 Workflow to Return the Appropriate Response Mode**
  This enhancement ensures that 3-legged OAM OAuth 2.0 workflow API (`/oauth2/rest/authorize`) returns the appropriate response mode `response_mode=form_post` if the consent expiry time has been set.
- **Support for Limiting PIN Generation During the Second Factor Authentication**
  New properties `MaxSendAttempts` and `MaxSendAttemptsLockoutEnabled` are added to the Adaptive Authentication Plugin to limit the PIN generation during the Second Factor Authentication. For details, see Limiting PIN Generation During the Second Factor Authentication.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.231005

Oracle Access Management 12.2.1.4.231005 BP includes the following new features and enhancements:

- **New Parameter to Fetch the Authorization Grant Details**
  Added a new parameter `response_mode` to fetch the authorization grants to `redirect_uri`. For details, see Table 39-7 Parameter Values for response_mode.
- **Support for Authentication in Multiple Browser Tabs**
  OAM supports multi-tab feature when `serverRequestCacheType` parameter is set to COOKIE. For details, see Supporting Authentication in Multiple Browser Tabs.
- **OAM OAuth2 Runtime Endpoint to Support Domain as a Query Parameter**
  A new query parameter `identityDomain` is added to the oauth2 runtime endpoint instead of the header parameter `X-OAUTH-IDENTITY-DOMAIN-NAME`. The header parameter `X-OAUTH-IDENTITY-DOMAIN-NAME` is not required when `identityDomain` is provided. If both parameters are used, `X-OAUTH-IDENTITY-DOMAIN-NAME` will take precedence over `identityDomain`. For details, see:
  - Create Access Token Flow
  - Introspect OAuth tokens
  - Revoke given access/refresh token
  - UserInfo details for OIDC flows
- **OAM OAuth2 Token Validation URL Supports Passing access_token both as a Header and as a Query Parameter**
  The `access_token` can be passed either as a header parameter or as a query parameter in the token validation URL. New syntax to initiate `access_token` as a header and as a query parameter are included in the REST API for OAuth. For details, see Validate Access Token Flow.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.230628

Oracle Access Management 12.2.1.4.230628 BP includes the following new features and enhancements:

- **Support for Administering a Secret Key**
  OAM supports administering a secret key using an access token with the BEARER authorization header by enabling the Secret Key Lifecycle feature.

  For more information, see Administering a Secret Key.
- **Access Token Exchange Support in OAM**
  Support for token exchange is made available in this release.

For more information, see Token Exchange Support in OAM.

- **OpenIdConnectPlugin plugin to Set Tokens as Session Responses**
  OIDC token values can be retrieved using policy authorization responses (header or cookie) using the following expressions:
  - For the access token: $session.attr.oidc.token.access
  - For the refresh token: $session.attr.oidc.token.refresh
  - For the ID token: $session.attr.oidc.token.id

  In a custom plugin, the following authentication context parameters can be used to obtain access token information:
  - token_response: full response from the token endpoint
  - access_token: access token value
  - refresh_token: refresh token value
  - idtoken: id token value
- **Functionality to Allow Cache Controlled by Request URL**
  Introduce an exception list to avoid caching of authorization policy results on Webgate specific resources. The following WLST commands are available for managing the exception list:

  ```
  configureWGAuthzCachingExceptionListUrls(noCacheURL, action)
  ```

  Example: `configureWGAuthzCachingExceptionListUrls("exceptionUrl", "add/remove")`
  - This WLST command can be used to add or remove URLs from the Webgate Authorization Caching Exception List on OAM Server.
  - '`action`' can be specified as '`add`' or '`remove`' to operate accordingly on `ExceptionList`

  ```
  configureWGAuthzCachingExceptionList(enabled, matchCriteria = "exactMatch", withQuery = "false")
  ```

  Example: `configureWGAuthzCachingExceptionList("true/false", matchCriteria = "exactMatch/startsWith", withQuery = "true/false")`
  - This WLST command can be used to enable or disable the Webgate Authorization Caching Exception List on OAM Server.
  - '`matchCriteria`' can be specified as '`exactMatch`' or '`startsWith`', with default being '`exactMatch`'
  - '`withQuery`' can be specified as '`true`' or '`false`', with '`false`' being the default meaning query-string from URL in Webgate authorization request will be ignored.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.220906

Oracle Access Management 12.2.1.4.220906 BP includes the following new features and enhancements:

- **Federation Partners Support Certificates Using RSASSA-PSS Signature Algorithms**
  OAM 12.2.1.4.220906 BP includes support for the Signature Algorithm SHA256-RSA-MGF1.

  > **Note:**
  >
  > This update is dependent on OWSM patch 34839859.

  For details, see Configuring RSA OAEP Key Transport Digest and MGF Digest.
- **The OAuth Client GET REST API is Enhanced to Retrieve the Client Secret**
  For use cases that require the administrators to display the client secret for registered clients in their admin portals. This feature needs to be enabled after applying the patch for the new behavior to take effect, so the secret for the clients that get registered after enabling this feature can be retrieved using the API. For existing clients that were registered before enabling the feature, the previous behavior of returning hashed secrets will continue.

  For details, see Manage OAuth Client Secret Retrieval.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.220404

Oracle Access Management 12.2.1.4.220404 BP includes the following new features and enhancements:

- **Make the OAM_ID Cookie Domain Scoped, Instead of Host Scoped**

  Support has been added to add a cookie domain for the OAM_ID cookie. This can be enabled by setting the configuration parameter `SSOCookieDomainEnabled` to true. The cookie domain for the cookie must be set through the configuration property `SSOCookieDomain`. These updates must be done in the `oam-config.xml` file using the import utility. A server restart is required after the import.

  For details, see bug 33291908 in Table 1-13.

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.220113

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

- **Support for OAuth Custom Claims Plugin**

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.210920

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

- **OAM SAML 2.0 Supported Encryption Algorithms**

  OAM supports AES-GCM encryption modes.

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

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

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

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

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

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

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

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

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

  For details, see Token Signing Using Third-Party Certificates.

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

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

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

- **Custom Claims**

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

For details, see Custom Claims.

- **OAuth Access Token Maximum Size**

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

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

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.210408

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

- **Session Management Optimizations**

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

  See also Database Tuning for Oracle Access Management in the *Tuning Performance Guide*.

- **OAuth Refresh Token Management**

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

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

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

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

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

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

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

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.201201

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

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

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

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

- **Keep the OAUTH_TOKEN Response Unset**

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

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200909

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

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

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

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

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

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

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200629

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

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

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

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

  Optional Configurations on OAM Server

  - If SSL/TLS is terminated on Load Balancer (LBR) and OAM server is not running in SSL/TLS mode, set the following system property in **setDomainEnv.sh**: `-Doam.samesite.flag.value=None;secure` Alternatively, you can propagate the 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 `$OAM_DOMAIN_HOME/bin/setDomainEnv.sh` and add the properties as shown below:

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

  3. Start the Administration and Managed Servers.

  Optional Configurations for WebGate

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

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

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

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

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

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

New Features and Enhancements in OAM Bundle Patch 12.2.1.4.200327

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

- **OAuth Consent Management**

  Provides the capability to manage and persist user consents while providing a mechanism to revoke them across Data Centers. The consent revocation capability is provided for both Administrators as well as individual users.

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

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

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

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

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

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

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

Understanding Bundle Patches

Describes Bundle Patches and explains 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 `Stack Patch Bundle for Oracle Identity Management Products (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.

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: 37684007
> - OINAV: 37054395
> - WLS Patch: 37714186
> - libovd: 36649916
> - EM: 36946553
> - ADF: 37769588
> - Coherence: 37658278
> - FMW Thirdparty Bundle: 37710654
> - 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:\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 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 p37882456_122140_Generic.zip
2. Unzip the patch zip file into the `PATCH_TOP`.

   ```
   $ unzip -d PATCH_TOP p37882456_122140_Generic.zip
   ```

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

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

```
"c:\Program Files\7-Zip\7z.exe" x p37882456_122140_Generic.zip
```

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

   ```
   $ cd PATCH_TOP/37882456
   ```

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\jdk180`

   > **Note:**
   >
   > OPatch operates on one instance at a time. If you have multiple instances, you must repeat these steps for each instance.
6. Start all Servers (AdminServer and all OAM Servers).

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

Use 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\p37882456_122140_Generic\37882
456
>c:\Oracle\oam12214\OPatch\opatch rollback -id 37882456
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/37882456`
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 37882456
   ```

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 12.2.1.4.250428

Resolved Issues in OAM Bundle Patch 12.2.1.4.250428

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

Table 1-1 Resolved Issues in OAM Bundle Patch 12.2.1.4.250428

Base Bug Number	Description of the Problem
37287932	ASDK ERROR - EXCEEDING SESSION LIMIT NUMBER
35929678	HARD CODED INDEX HINT CAUSING SQL PERFORMANCE REGRESSION FOR BUGFIX 35591710
37208431	FORGOTPASSWORD WITH OTP DOESN'T REDIRECT TO LOGIN IF SERVERREQUESTCACHETYPE=FORM
37383063	ATTRIBUTE LATESTOTPDATASFAPIN WHICH IS NOT ALLOWED BY ANY OF THE OBJECTCLASSES
37139250	OAM 12CPS4: CONSENT/REVOKE API NOT RETURNING ATTRIBUTE TOKENREVOKETIMESTAMP WITH OCTOBER BP :37131265

Table 1-1 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.250428

Base Bug Number	Description of the Problem
37321460	PASSWORD RULES ARE NOT DISPLAYING IN DUTCH IN PASSWORD RESET FLOW
37390421	OAM 12CPS4: DIFS IN MDC OAUTH TOKENEXCHANGE MODULE WITH JAN BP :37349292
37444780	CVE-2024-52046
37389548	ACCESS TOKEN FOR MULTIPLE SCOPE ID IS NOT WORKING IN OCT BP 2024
37172574	THE /OAUTH2/REST/TOKEN/INFO API CALL FAILS WITH "ERROR": "UNAUTHORIZED_CLIENT"
37365624	OAUTH PERFORMANCE ISSUE
37268882	12C ACCESS TOKEN: CUSTOM ATTRS WITH EMPTY VALUE SHOULD NOT BE DISPLAYED IN **Note:** Set the following system property in the setDomainEnv.sh to enable the feature `oracle.oam.oauth.custom.claim.value.not.found=true`
37366665	UNABLE TO CREATE AND PERSIST USER SESSION ON LARGE SAML ATTRIBUTES
37121369	OAUTH/OIDC REST API ISSUES WITH DISPLAY CLIENT INFORMATION
37171265	SOME CHANGE PASSWORD RULES ARE URL-ENCODED ON THE RESET PASSWORD PAGE Added a new system property: - `Doracle.oam.rules.special.characters.allowed=<special character>`
37276108	WS-FEDERATION ACTIVE PROFILE SUPPORT ISSUER URL AND IMMUTABLE ATTRIBUTE MAPPING SHOULD BE CONFIGURABLE
36846382	SET RESPONSE HEADERS TO VALUES OBTAINED PROGRAMMATICALLY
37226073	WS-FEDERATION ACTIVE PROFILE SUPPORT FOR OAM

Resolved Issues in OAM Bundle Patch 12.2.1.4.241227

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

Table 1-2 Resolved Issues in OAM Bundle Patch 12.2.1.4.241227

Base Bug Number	Description of the Problem
36834063	WLST SAVEACCESSARTIFACTS AND DOWNLOADACCESSARTIFACTS DISPLAY OAM SCHEMA PASSWORD
37205986	ERROR IN MAPPING NEW OAUTH DOMAIN CERT VIA END POINT - KEYPAIRADMIN/KEYPAIR
35730510	OAM12C: FMWCONFIG\KEYSTORES.XML GETS TRUNCATED WITH ADMINSERVER RESTART
37056339	INCORRECT ERROR THROWN FOR LDAPCONNECTIONEXCEPTION ERRORS
37143199	OAM 12C - USERPASSWORDCHANGECHECKENABLE GENERATES NPE WHEN USED WITH IDS PROFILE
36404773	PKCE ISSUE AFTER OAM PATCHING
37166257	Fix for Bug 37166257
36607545	OAM SESSION SUPPORTS ONLY 5 LARGE ENCODED OBJECTS
37041275	APRIL 24 BP: ERROR ON LOGIN WHEN LANGUAGE PICKER IS ENABLED AND ADAPTIVE MODULE IS USED
36928507	GETPARTNER API AFTER UPDATING THE PARTNER DETAILS IS NOT RETURNING FEW PARAMETERS OF PARTNER
37164042	QUERY PARAMETERS STRIPPED FROM BACKURL AFTER PASSWORD CHANGE
36117541	WEBSERVER HOST ADDED AS INVALID AGENT TO MONITORING TOOLS AFTER UPGRADE TO PS4 The following system property must be set to false in `setDomainEnv.sh` file to use this feature: `-Doracle.oam.agent.unknown=false`
36963201	CUSTOM SESSION ATTRIBUTES ARE MISSING AFTER JULY BP
36978601	FORGOT PASSWORD LINK IN CHANGING THE LANGUAGE DOES NOT WORK FOR DUTCH
36903429	SOME CHANGE PASSWORD RULES ARE URL-ENCODED ON THE /OTPFP/INITCHANGEPSWD PAGE
37032960	OPTION TO HAVE ONE AUDIENCE DEFINED IN A JWT TOKEN IN 3-LEGGED
36537244	JAVA.LANG.EXCEPTIONININITIALIZERERROR ON CUSTOM CONSENT PAGE

Resolved Issues in OAM Bundle Patch 12.2.1.4.241009

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

Table 1-3 Resolved Issues in OAM Bundle Patch 12.2.1.4.241009

Base Bug Number	Description of the Problem
36988215	DCC TUNNELING NOT WORKING WITH14.1.2.0.0 WEBGATE
22086890	Fix for Bug 22086890
36698101	SOAP ERROR AFTER APPLYING 36268742 WHEN ARTIFACT BINDING IS ENABLED
36800770	FORGOT PASSWORD FLOW FAILING DUE TO THE OLDER JACKSON DEPENDENCY
36304146	THREAD DUMPS FROM ORACLE.OAM.PROXY.OAM LOGGER
36783960	OAM - CHANGES TO SUPPORT 14C DCC WEBGATES
36500395	IDP DISCOVERY SERVICE "DISCOVERY.JSP" ADDING PREFIX "/OAMFED/" TO THE RETURN URL
30674068	UNABLE TO CHANGE OAUTH AUTHZ CODE EXPIRYTIME FROM THE HARDCODED 5 MINUTE VALUE
35313268	ENH - OPENID - NEW ID TOKEN TO BE PROVIDED WHEN USING THE REFRESH TOKEN
26417358	Fix for Bug 26417358
19988352	Fix for Bug 19988352
34381899	Fix for Bug 34381899
36975884	PLUGINS TO FACILITATE MFA WITH OAA
36789669	OAM RESOURCE PASSWORDLESS FLOW FAILS WITH SYSTEM ERROR
36734401	CHIPS CONFIG DEPENDENCY ENHANCEMENT
36666715	PARTNER KEY UI OPTIMIZATION
36248319	OAM COOKIES BLOCKING IFRAMING FA PAGE IN VB
36124197	AUTOMATIC REUSE DETECTION OF OAUTH TOKENS
16315022	Fix for Bug 16315022
36805629	OAUTH ACCESS TOKEN AUD CONTAINS AUTHORIZATION SERVER URL IN A 2-LEGGED FLOW The following system property must be set to `false` in `setDomainEnv.sh` file to use this feature `-Doracle.oam.oauth.at.audience.default=false` By default the system property value is `true`.
36739991	WRONG ALGORITH DISPLAYED ON THE .WELL-KNOWN/OPENID-CONFIGURATION URL
36724949	OTP PASSWORD RESETS FAILS AFTER APPLYING APRIL 2024 CPU PATCHES

Table 1-3 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.241009

Base Bug Number	Description of the Problem
36766496	ORA-14300: PARTITIONING KEY MAPS TO A PARTITION OUTSIDE MAXIMUM PERMITTEDNUMBER
36694433	FAILEDCOUNTFIELD NOT UPDATED FOR OMA FLOW
36268742	OAM SOAP FAULT RESPONSES MISSING ENVELOPE

Resolved Issues in OAM Bundle Patch 12.2.1.4.240701

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

Table 1-4 Resolved Issues in OAM Bundle Patch 12.2.1.4.240701

Base Bug Number	Description of the Problem
36714022	ANDROID PUSH NOTIFICATION MFA : CHANGES IN GOOGLE FCM API FOR PUSH NOTIFICATION FLOW
36534269	AFTER JAN OR APR 20 IDM SPB 24 OAM MFA SMS PHONEMASKREGEX STOPS MASKING
36416361	ABLE TO AUTHENTICATE WITH OMA WHEN ACCOUNT IS LOCKED
33471957	ER: OAM 12.2.1.4 - REQUEST RS512 TOKEN SIGNING ALGORITHM FOR OAUTH
36345002	REVOKING OAUTH TOKEN BY MTLS CLIENT FAILS WITH "INVALID CLIENT CREDENTIALS"
36502257	INVALID INPUT USING COLON IN RESOURCESERVERNAMESPACEPREFIX FOR OAUTH SCOPES
36015259	PUBLICCLIENTREFRESHTOKENENABLED & GRANTTYPEREFRESHTOKENENABLED VISIBLE IN CLAIM
36103252	CVE-2020-13956

Note:

The following system property must be set to `true` in `setDomainEnv.sh` file to use this feature.

- `Doracle.oam.oauth.allow.all.char=true`

Table 1-4 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.240701

Base Bug Number	Description of the Problem
36416071	OAM 12CR4 - OTP AUTHENTICATION FAILS AFTER APPLYING JANUARY SPB PATCH 36179836
36495989	OAUTH TOKEN INFO ENDPOINT IS NOT RFC COMPLIANT **Note:** The following system property must be set to `true` in `setDomainEnv.sh` file to use this feature. – `Doracle.oam.oauth.at.format.rfc=true`
36022806	WITH ENABLEEXTRASAMLATTR SET TRUE , SESSION SHOULD SUPPORTS MORE THEN 40 STRING TYPE PROPERTIES
36172877	FEDERATION PROXY ENABLED FLOW : AUTHENTICATED FEDERATED USER SHOULD BE PASSED TO USERIDENTIFICATIONPLUGIN **Note:** The following system property must be set to `true` in `setDomainEnv.sh` file to use this feature. – `Doam.federationProxyEnabled=true`
36565740	14.1.2:OAMCONSOLE ACCESS VIA OHS RETURNS OPERATION ERROR IN HA SETUP
36268857	IOS PUSH NOTIFICATIONS DO NOT WORK WITH THE JAN 24 BP RELEASE
36293695	UPDATE OAUTH CLIENT UPDATES CLIENT SECRET
36410353	OAM FAILS WHEN BROWSER SENDS 2 OAM_ID COOKIES

Resolved Issues in OAM Bundle Patch 12.2.1.4.240328

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

Table 1-5 Resolved Issues in OAM Bundle Patch 12.2.1.4.240328

Base Bug Number	Description of the Problem
36413066	LEVERAGE THE SESSION VALIDATE END-POINT TO REGENERATE OAM_RM TOKEN BASED ON A TAP TOKEN
35299815	REMOVE THE ABILITY TO CREATE/EDIT OAM SERVERS OR WEBGATE AGENTS IN SIMPLE MODE
36282327	WEBGATE AGENT REGISTRATION INSTALLS EXPIRING SIMPLE CERTIFICATES INTO THE AGENT ARTIFACTS
36408603	API KEY LIFECYCLE OPTIMISATION
36424469	API KEY UI OPTIMIZATION - UI BUG FIX
36277851	CVE-2019-0231
36408621	API KEY UI OPTIMIZATION
36277847	OAM AUTHENTICATION API FOR OUA NEEDS TO RETURN PASSWORD POLICY RELATED CODES
36377223	ID_TOKEN SUPPORT WHILE CREATING DOMAIN
36103295	CVE-2022-24329
36362711	DOMAIN RETRIEVAL FAILS AFTER ROLLBACK
34906532	INVALIDATE ACCESS TOKEN IF USERS PASSWORD IS UPDATED
33806048	ER - POSSIBILITY OF USING 2 CERTIFICATES AT THE SAME TIME IN FEDERATION
35984683	OAUTH CLIENT SECRET EXPIRATION AND ROTATION
36336356	NPE IS THROWN WHILE GENERATING access_token and id_token USING MULTIPLE FLOWS
36252694	CUSTOM CLAIMS NOT PRESENT IN ACCESS TOKEN FOR IMPLICIT GRANT_TYPE
35194455	ER - OPTION TO CUSTOMIZE THE ISSUER DISCOVERY IDENTIFIER AND ISS TOKEN CLAIM
35662872	LONGER VALABILITY FOR ID_TOKEN THAN ACCESS_TOKEN
35188279	MASK SAML RESPONSE ATTRIBUTES IN OAM LOG MESSAGE
34911587	CONSENT PAGE THROWS ERROR IF THE END USER DELAY TO APPROVE 5MIN
34840243	CHECK AUTHENTICATIONCONTEXT WHEN OAM IS ACTING AS SP
36090820	OBLOGINTRYCOUNT UPDATES INCONSISTENT FOR DEACTIVATED USER

Table 1-5 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.240328

Base Bug Number	Description of the Problem
36129573	MDC OAUTH CONSENT MANAGEMENT FAILS IF MASTER DC IS DOWN AFTER OCT 2023 PS4 BP **Note:** In the MDC Clone set the following system property to `true` in `setDomainEnv.sh` - `DfailOnConsentStoreError=true`
35946569	OAUTH RESOURCE SERVER CREATION FAILS WITH SPECIAL CHAR IN ANY FIELD **Note:** The following system property must be set to `true` in the `setDomainEnv.sh` - `Doracle.oam.oauth.allow.all.char=true`
36264952	1412 soa sso logout issue after integration with 1412 OHS/ 12214 OAM for SSO

Table 1-5 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.240328

Base Bug Number	Description of the Problem
36029627	OAM OAUTH: STATE PARAMETER IN CALLBACK URL GET ENCODED IN 12CR2 PS4
35854499	OAM 14C ENT: OAM NEEDS TO SUPPORT MD5 HASHING FOR LEGACY WEBGATES
21271197	MULTIPLE ROWS FOR OAMS.OAM_OAM METRIC WHILE RETRIEVING AUTHENTICATION REQUESTS

Note:

- The following system property must be set to `true` in `setDomainEnv.sh` file to use this feature.

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

  By default the system property is false.
- This is relevant only when state parameter contains URI safe character according to the URI RFC. For more details, see https://datatracker.ietf.org/doc/html/rfc3986#section-2.2.

Resolved Issues in OAM Bundle Patch 12.2.1.4.240109

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

Table 1-6 Resolved Issues in OAM Bundle Patch 12.2.1.4.240109

Base Bug Number	Description of the Problem
35986960	OAUTH 2.0 RUNTIME API ENDPOINTS SHOULD SUPPORT IDENTITYDOMAIN IN FORM PARAMETERS ALSO
35790270	OAM12C TIME SESSION
35776509	REST API NOT SHOWING CERTIFICATE EXPIRATION DATE FOR MANUALLY CONFIGURED PARTNER
35974882	OAUTH 2.0 AUTHORIZE 3L ENDPOINT INCORRECTLY RETURN IN QUERY MODE WHILE RESPONSE_MODE=FORM_POST IS REQUESTED IF "CONSENTEXPIRYTIMEINMINUTES" DOMAIN CUSTOM ATTRIBUTE IS SET
35777407	OIDC: SUPPORT OF "RESPONSE_MODE" NEEDED IN THE "AUTHORIZATION CODE GRANT FLOW"
35820991	EMAIL_VERIFIED CLAIM IS BOOLEAN BUT ID_TOKEN RETURN IT AS STRING
35798094	CVE-2023-3635
35798089	CVE-2021-0341
35823067	SCOPE NAME WITH : WORKS WITH POST TO ADD BUT NOT WITH PUT / UPDATE
35840877	OTP NOT WORKING FOR NEW USERS POST PATCHING WITH ER 34394159
35952776	NULL CHECKS NEED TO BE ADDED FOR PROGRAMMATIC AUTHN REST INTERFACES
35437597	OAM 12CPS4 - WITH ER 35186662 ID_TOKEN VALUE IN HEADER/COOKIE RESPONSES IS NOT BASE64 ENCODED
35943082	PROVIDE REST INTERFACES FOR PROGRAMMATIC AUTHN LEVERAGING OAM RM TOKEN
31471722	[ER] NEED REFRESH TOKEN RESPONSE WHEN MAKING A GRANT_TYPE=REFRESH_TOKEN OAUTH
35650808	IS REFRESH TOKEN RETURNED IN WHEN USING MOBILE_CLIENT AS A CLIENT TYPE
35786620	HANDLING OF SYSTEM ERRORS UNDER DIFFERENT MFA FLOW ERRORS FROM OAA TO OAM
35745907	PIPELINE DELIMITER BREAKS FEDERATION
35896603	USERS ENCOUNTERS RUNTIME ISSUES AT MFA
35854158	Fix for Bug 35854158
34394159	OAM 12C - NEED AN OPTION TO LIMIT THE NUMBER OF TOTP GENERATED

Resolved Issues in OAM Bundle Patch 12.2.1.4.231005

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

Table 1-7 Resolved Issues in OAM Bundle Patch 12.2.1.4.231005

Base Bug Number	Description of the Problem
34162278	IMPLICIT GRANT FLOW OIDC USERSCOPE DATA TO BE MADE AVAILABLE THROUGH PAYLOAD
35480610	GETSESSIONINFORESPONSE BREAKS IN CLUSTER ENV, IF IDSTOREREF IS EMPTY
35327681	DIAG: NEED TO LOG BELOW ERROR AT WARNING LEVEL
35315633	SERVICE MANAGER APPLY API TIME IMPROVEMENT TO APPLY CHANGES IMMEDIATELY AND THREAD SAFE
35605163	OAM 12C - TYPO IN OIDC PLUGIN: OUATH_CLIENT_SECRET INSTEAD OF OAUTH_CLIENT_SECRET
35591710	INVALID HINT IN APPLICATION SQL OR INVALID INDEX NAME ON AM_SESSION RELATED INDICES
35250383	MISSING BROWSER TYPE INFORMATION INTO AUDIT DATABASE TABLE OAM 12C ENV
35504810	OAUTH: SESSION_ID CLAIM FROM JWT TOKEN NOT MATCHING SESSION_ID FROM OAM SERVER
35692992	OAA PLUGIN ATTR VALUE SEND TO OAA TO BE USED AS EXTERNAL_ID IS NOT CONFIGURABLE
35386271	OOTB CERTIFICATE STILL VISIBLE AFTER CONFIGURING 3RD PARTY KEY PAIR
35269389	TOKEN VALIDATION: PASSING ACCESS_TOKEN AS A HEADER INSTEAD OF QUERY PARAMETER
28461556	X-OAUTH-IDENTITY-DOMAIN-NAME AS QUERYPARAMETER TO OAM12C ACCESS TOKEN END POINT
35552946	OPENIDCONNECTPLUGIN : OAUTHTOKEN NOT GENERATING AND NOT SETTING KEY_USERNAME
35470456	LOGOUT USING CUSTOM PAGE FAILED W/ MALFORMED URL W/ RETURNURLVALIDATIONENABLED
35327246	OAUTH SSO LINKING : ACCESS TOKEN IS VALIDATED AFTER SESSION TIMEOUT

Note:

In the Custom OIDC Authentication Module , make sure `donotpassclientid=true` is set in the additional attributes of `openidconnectPlugin`.

Table 1-7 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.231005

Base Bug Number	Description of the Problem
35217506	CVE-2021-37136
35509441	OIDC PLUGIN NOT SETTING KEY_USERNAME
35208828	ENH - NEED THE SOLUTION FROM BUG 30267123 FOR SERVERREQUESTCACHETYPE=COOKIE
35515193	COULD NOT GET THE DECRYPTING SYMMETRIC KEY, GOT PRIVATE KEY INSTEAD **Note:** For this fix set the following parameter: - `Doracle.oam.fed.isAdviceIgnoreEnabled=true`
34820203	PASSWORD CHANGE PAGE ISSUE FOR SPECIAL CHARACTERS RESTRICTION
35371374	POLICY CACHE AUDIT EVENTS SHOULD DISPLAY POLICY DETAILS
34760767	ACCESS TOKEN GENERATED WITHOUT A CONSENT
34868608	COMMON CRITERIA - NULL CIPHER DURING TLS HANDSHAKE CAUSES CPU TO SPIN
32406872	PKCE : OAM DOES NOT VALIDATE THE CODE GENERATED WITHOUT PADDING
35724621	OAA AND OAM INTEGRATION AND INSTALLATION AND ACCESS OF OAAADMIN-UI AND SPUI ACCESS INCONSISTENCIES

Resolved Issues in OAM Bundle Patch 12.2.1.4.230628

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

Table 1-8 Resolved Issues in OAM Bundle Patch 12.2.1.4.230628

Base Bug Number	Description of the Problem
35194283	SAML:AUDIENCE AS MULTI-VALUE AND NOT AS LIST

Table 1-8 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.230628

Base Bug Number	Description of the Problem
34634700	IDP DISCOVERY SERVICE FAILS WITH 'INVALID OR NULL RESPONSE URL' **Note:** For this fix set the following parameter: - `Doam.federationProxyEnabled=false`
35198097	AFTER APPLY DEC-2022 OAM BP SUITE THE MDC APS BLOCKED
34556443	JBO-25006: INDEX OUT OF RANGE WITH A LARGE NUMBER OF ENCRYPTION KEYS IN ADMIN C
34018795	FUNCTIONALITY TO ALLOW CACHE CONTROLLED BY REQUEST URL
35205538	PASSWORD CHANGE PAGE NOT RENDERING PROPERLY IF NEW PASSWORD DOES NOT MEET SPECIAL CHARCTER RULE
35205593	PASSWORD RULES ARE MISSING IN CHANGE PASSWORD PAGE
27918612	SAML ATTRIBUTE VALUE IS NULL WHEN ONE OF THE USER ATTRIBUTE VALUE IS NULL IN COM
32804378	OAM / OAUTH IMPERSONATION & DELEGATION SUPPORT (RFC8693)
35131903	OAUTH TOKEN ONLY CONTAINS 'GRANT' CLAIM FOR AUTHZ CODE GRANT TYPE **Note:** `enableDisplayGrantType` custom attribute must be set to true in the OAuth identity domain to enable the grant type in the access token. By default it is set to false.
35112063	SP ATTRIBUTE PROFILE MAPPING : USER ATTRIBUTE CASING ISSUES

Table 1-8 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.230628

Base Bug Number	Description of the Problem
35080285	"JDBCLOCATEEXCEPTION: FAILED TO LOCATE USER" AFTER UPGRADING TO 12.2.1.4
35186662	OPENIDCONNECTPLUGIN PLUGIN SHOULD SET TOKENS AS SESSION RESPONSES
34911015	UNABLE TO RETRIEVE THE OAUTH SECRETKEY USING THE REST APIS
34092777	CVE-2020-36518

Resolved Issues in OAM Bundle Patch 12.2.1.4.230317

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

Table 1-9 Resolved Issues in OAM Bundle Patch 12.2.1.4.230317

Base Bug Number	Description of the Problem
35012645	Fix for Bug 35012645
34866912	NULL POINTER EXCEPTION AFTER USING 34085191 WITH BP12
34979560	USERID WITH SPECIAL CHARACTER }) COMBINATION FAILED TO AUTHENTICATE TO OID
35058183	OAM 12C - OAUTH CERTIFICATE IS USING KEY_OPS=SIGN INSTEAD OF KEY_OPS=VERIFY
35117017	Fix for Bug 35117017
35119994	USERAUTHENTICATIONPLUGIN NULLPOINTEREXCEPTION PASSWORD GRANT FLOW PATCH 34791593

Note:

The following Java parameter must be set to `true` in `setDomainEnv.sh` to enable escaping of special characters: `-Doam.escapeSpecialChar.enable=true`.

By default this property is set to `false`.

Table 1-9 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.230317

Base Bug Number	Description of the Problem
35066999	X5T AND X5T#S256 DIGESTS FOR /OAUTH2/REST/ SECURITY ARE NOT RFC COMPLIANT **Note:** • A new system property `oracle.oauth.security.x5t.withoutpadding=true` is added. The default value of this system property is `false`. • The following Java parameter must be set to `true` in `setDomainEnv.sh` to enable this feature: `-Doracle.oauth.security.x5t.withoutpadding=true`. By default the parameter is set to `false`.
35008348	Fix for Bug 35008348
34616152	OOTB JPS-CONFIG.XML HAS SYNTAX ERROR
32598824	OAM 12CPS3: LOGIN TO PROTECTED RESOURCE AFTER GLOBAL SESSION IDLE TIME OUT USING DIFFERENT USER ACCOUNT DETAILS IS NOT ALLOWED
34831878	ARTIFACTS ARE NOT PUSHED TO DB WHEN ADMIN SEVER IS STARTED FIRST TIME WITH 12CPS4
34987409	OAUTH REST-API DOES NOT LIST GRANTTYPES WITH ACCEPT: APPLICATION/JSON
35008310	Fix for Bug 35008310
34994891	USER HAS ALREADY EXISTING SESSION WITH SESSIONID AFTER TIMEOUT

Table 1-9 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.230317

Base Bug Number	Description of the Problem
34791593	PLUGIN EXECUTION FAILS WHEN INITIAL_COMMAND=NONE IS USED DURING STEP-UP **Note:** You should add the parameter `plugin_stepup_flow=ON` along with `INITIAL_COMMAND=NONE` to the authentication scheme parameter section. The OAM plugin then checks whether the `OAM_ID` cookie is present and the user has been authenticated. If present, the flow checks whether it matches the authenticated user and then the plugin returns success.
34727970	/OAUTH2/REST/TOKEN/INFO ENDPOINT RESPONSE DO NOT COMPLY JSON FORMAT FILE **Note:** The following Java parameter must be set to `false` in `setDomainEnv.sh` for this fix to work. – `Doracle.oam.oauth.allow.escape=false`. By default it is set to `true`.
34718515	PASSWORD CHANGE PAGE ISSUE FOR OAM SSL AND SPECIAL CHARACTERS RESTRICTION
34881208	END USER/SOURCE SYSTEM IP NOT PRESENT IN FED AUDIT LOGS

Table 1-9 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.230317

Base Bug Number	Description of the Problem
34676152	OAM_REMOTE_USER HEADER IS GETTING SET TO USER CN INSTEAD OF UID

Resolved Issues in OAM Bundle Patch 12.2.1.4.221208

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

Table 1-10 Resolved Issues in OAM Bundle Patch 12.2.1.4.221208

Base Bug Number	Description of the Problem
34847202	Fix for Bug 34847202
34734586	Fix for Bug 34734586
34765801	DIAG: "REQUIRE TO APPLY LIBOVD PATCH#33368783" MESSAGE EVEN THOUGH PATCH IS APPLIED
33327287	SIMPLE MODE GLOBAL PASSPHRASE UPDATE DOES NOT PUSH NEWLY GENERATED ARTIFACTS TO DB
34350022	APP DOMAIN TIME OUT NOT WORKING FOR ADAPTIVEAUTHNSCHEME
34670445	CUSTOMIZE LOGOUT PAGE ON MDC FEDERATED PROXY ENVIRONMENT
34728321	12.2.1.4 OCT 2022 BP BREAKS FEDERATED LOGINS WHEN SHA-256 IS USED
34756122	HIGH CPU IN PRODUCTION OAM SERVER WHEN USERNAME IS EMPTY IN USERIDENTIFICAIONPLUGIN
34282474	RELOGIN DOES NOT REDIRECT TO SUCCESS URL AFTER LOGOUT
34550841	LOGOUT ADDS A QUESTION MARK CHARACTER TO THE LOGOUT TARGET URL
34639003	FED IDP FAILS WHEN LOADING /OAMFED/ POSTPROFILE.JSP
34461263	OAM SESSION SUPPORTS ONLY 10 ENCODED SUBJECT STRING TYPE PROPERTIES
34451944	OAUTH AUTHZ FAILS IF WNA FALLBACK FORM IS ENABLED AND STATE PARAM IS VERY LONG

Table 1-10 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.221208

Base Bug Number	Description of the Problem
34483288	WHILE USING OAUTH ENDPOINT THE REDIRECT URL IS ENCODED TWICE **Note:** The following Java parameter must be set in `setDomainEnv.sh` to enable this feature: -`Doracle.oam.oauth.redirecturi.decode=true`
34530517	UNABLE TO RESET PASSWORD OR CONTINUE AFTER PASSWORD WITHIN WARNING PERIOD
34636811	OAM JIT : DISPLAYS THE CONTENT OF HTML FILE USED IN AUTHENTICATION SCHEME IN USER AUTO-PROVISIONING WITH PASSWORD PROMPT FLOW
34501342	OAUTH CUSTOM CLAIMS PLUGIN SUPPORT FOR 'REFRESH_TOKEN' GRANT_TYPE
34456006	OAM_RES STILL APPEARS WHEN AUTHZCALLBACKENABLED IS SET TO FALSE
34298417	OAUTH :VALIDATE TOKEN API : CONSENT CREATION TIME IS AFTER LDAP RESPONSE READ TIMED OUT **Note:** • The LDAP response read timeout used here is 10000 seconds. • Set the -`Doam.oauth.token.validation.clock.skew` parameter in `setDomainEnv.sh` to a value that is appropriate for the your environment.

Resolved Issues in OAM Bundle Patch 12.2.1.4.220906

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

Table 1-11 Resolved Issues in OAM Bundle Patch 12.2.1.4.220906

Base Bug Number	Description of the Problem
34411580	LDAP ATTRIBUTE NOT CAPTURED IN COOKIE USING PREFETCH
34085191	SETSPPARTNERDEFAULTSCHEME() FAILS FOR NEW AUTHN SCHEMES IF POLICY MGR IS UP
34461370	Fix for Bug 34461370
34020728	OAM 12CPS4: /OAUTH2/REST/USERINFO RETRIEVING 400 RESPONSE CODE IF AUTHZ CODE GENERATED WITH CUSTOM AND OPENID SCOPES
32960094	SUPPORT FOR CUSTOM ATTRIBUTES IN SAML RESPONSE **Note:** The following system property must be set in `setDomainEnv.sh` to enable this feature: – `Doam.saml.customattr=true`
34373383	Fix for Bug 34373383
34469057	JSON FORMAT WHILE LISTING ALL THE IDENTITY DOMAINS
34359848	OAM AS IDP FAILS WITH SSO SESSION IS NULL OR INVALID
34353017	OAM 12C SYSTEM ERROR AFTER 15 MINS(DEFAULT REQ TIMEOUT) PASSED ON LOGIN PAGE
34467460	OAUTH FLOW BREAKS WHEN REDIRECT URL CONTAINS "?"
31916721	OAUTH :12CPS4 : CLIENT SECRET: NOT ABLE TO VIEW \ RETRIEVE
34247621	GREEK LETTERS IN IN GROUP NAME BREAK OAM - ADAPTIVE AUTHENTICATION RULE
33629727	AUTHENTICATION MODULES MISSING ON CLONE
34223066	OAM SERVER: MDC : COUPLE OF ERRORS ARE FLOODING THE LOGS
34403516	OAM DOES NOT THROW INVALIDMETADATAFILEEXCEPTION WHEN KEYINFO CORRUPTED IN PARTNER METADATA

Table 1-11 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220906

Base Bug Number	Description of the Problem
34241746	APP DOMAIN LAST ACCESS TIME NOT UPDATING RESULTING IN UNEXPECTED IDLE TIMEOUTS
34234548	OAM_LOGOUT_CALLBACK_URLS NOT GETTING INVOKED WITH 12CPS4 DCC WEBGATES UNLIKE 11G WEBGATES
34187283	MULTIVALUEGROUPS DOES NOT WORK PROPERLY WHEN FEDERATION IS ACTING AS PROXY For federation proxy use cases, if a multi-valued attribute returned by an Identity Provider (IdP) needs to be sent back to the Service Provider (SP) as a multi-valued attribute, the following configuration must be done from the OAM console. • Add a mapping in the IdP attribute profile to map a multi-valued attribute with a name containing `oam.multivalued`. For example, `oam.multivalued.<attrName>` • In the SP attribute profile of a federation proxy, add an attribute name mapping of `$session.attr.fed.attr.oam.multivalued.<attrName>`
34238089	OAM REST API EXPECTING AUTHORIZATION HEADER ON PREFLIGHT OPTIONS CALL
34060169	ORA-01878 CAUSING PARTITIONS COUNT TO INCREASE IN 100S IN PROD
34049361	NEED 28228295 TO COVER 'CLIENT_CREDENTIALS' GRANT_TYPE
34149570	FAILONCONSENTSTOREERROR : NOT WORKING FROM BP 06 ONWARD
34142447	STORAGE NOT CONFIGURED ERROR MESSAGE IN DETAILED SESSION SEARCH OAM 12C
34020168	GETTING XMLSTREAMEXCEPTION IN OAM STARTUP LOG AFTER DEPLOYING CUSTOM WAR
32927966	OAM SP DOES NOT KNOW SIGNATURE ALGORITHM SHA256-RSA-MGF1 IN SAML RESPONSE

Note:

This bug is dependent on OWSM patch 34839859.

Resolved Issues in OAM Bundle Patch 12.2.1.4.220623

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

Table 1-12 Resolved Issues in OAM Bundle Patch 12.2.1.4.220623

Base Bug Number	Description of the Problem
33843455	OAM 12.2.1.4 - OAUTH CLIENT APP FAILS WITH ERROR - STATE STRING NOT VALID
33822933	12CPS3 : PROFILE EMAIL CLAIM ATTRIBUTE MAPPING
33752393	OAMREAUTHENTICATE IS PASSING ON URLS IN QUERY STRING IN DECODED FORMAT **Note:** You can enable the fix by adding the following Java parameter in `setDomainEnv.sh`: `-Doracle.oam.proxy.queryStringDecoding=false`.
34031691	PASSWORD RULES NOT DISPLAYED IN FR_CA
33901539	SYSTEM ERROR WHEN CUSTOMER TESTING SSO WITH CORNERSTONE IDP
27050584	HOW TO MAKE IDP DN MAPPINGS CASE INSENSITIVE WITH 11.1.2.3 FEDERATION
33735897	USERPRICIPALNAME IS EXTRACTED WITH SPECIAL CHARACTERS FOR SOME USERS WHILE USING THE X509 AUTHENTICATION
33837000	CONFIGUREPOLICYRESPONSES DOES NOT WORK AS EXPECTED **Note:** You can use this feature by adding the following Java property in `setDomainEnv.sh`: `-Doam.fed.attr.isReplaceBackslashComma=true`
34088890	MFA OTP AUDIT

Resolved Issues in OAM Bundle Patch 12.2.1.4.220404

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

Table 1-13 Resolved Issues in OAM Bundle Patch 12.2.1.4.220404

Base Bug Number	Description of the Problem
33856331	PASSWORD RULES NOT DISPLAYED IN FRENCH
33814292	REMOVING UNUSED LOGGING DEPENDENCIES
33409018	NEED HINTS FOR 2 OAM SQLS USED FOR DB SME SO AS TO USE CORRECT INDEXES
33417041	OAM/SERVICES/REST/ACCESS/API/V1/AUDIT/EVENTS 500 ERROR
32910834	12CPS5 RUP: FILE NOT FOUND EXCEPTIONS IN EXPORT_OFFLINE_OIM AND IMPORT_OFFLINE_OIM
32587773	Fix for Bug 32587773
33724245	TO SUPPORT THE ALLOW LIST FEATURE IN ORDER TO ENABLE EMBEDDING IN A FUSION APP IFRAME
33841128	MAKE OAA PLUGIN AN OOTB PLUGIN
33913030	USE SYSTEM->GETPROPERTY TO READ SYSTEM PROPERTY OAM.T2P.ENABLETOPOLOGYUPDATE
33663608	USERINFO ENDPOINT : RETURSN VALUES FOR REVOKED ACCESS TOKEN
33645782	OAM12C: UNABLE TO MODIFY AUTHN SCHEME WITH CHALLENGE MECHANISM OAM10G USING CURL
33478014	ERRORS/WARNINGS SEEN ON STARTING SERVERS AFTER OAM 12C

Table 1-13 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220404

Base Bug Number	Description of the Problem

33291908	MAKE THE OAM_ID COOKIE DOMAIN-SCOPED, INSTEAD OF HOST SCOPED
	The following configuration properties are introduced in oam-config.xml:
	• `<Setting Name="SSOCookieDomain" Type="xsd:string">.mydomain.com</Setting>`
	• `<Setting Name="SSOCookieDomainEnabled" Type="xsd:boolean">true</Setting>`
	To set the domain for `OAM_ID` cookie perform the following steps:
	1. Search for `SSOCookieDomainEnabled` in `oam-config.xml`.
	2. Change the value to true.
	`<Setting Name="SSOCookieDomainEnabled" Type="xsd:boolean">true</Setting>`
	`<Setting Name="SSOCookieDomain" Type="xsd:string">.mydomain.com</Setting>`
	Note:
	If `SSOCookieDomainEnabled` is not already present then add the `<Setting Name="ssoengine" Type="htf:map">` setting before setting the `SSOCookieDomainEnabled` value to true.
	3. Restart the OAM server.

33021500	ASDK FAILS TO CONNECT TO RUNNING OAM SERVER
33466152	JAVA.LANG.CLASSNOTFOUNDEXCEPTION AFTER OAM UPGRADE: KM 2806412.1 If the configured SME store is not DB then add the following Java property in the `setDominEnv.sh`: `-DDB_SMESTORE_SYSPROP=false`
33556093	AFTER APPLYING FIX FOR BUG 30771422 STILL WARNING ENTRIES ARE SPAMMING THE LOGS If you are using advanced authentication rules containing requestMap[Cookie] then add the following system property in the `setDomainEnv.sh`: `-Doam.rule.requestAttr=Cookie::NULL_VALUE`
33604330	ERRORS WHEN LOADING IPFWARNINGMSG.JSP & IPFPSWDCHANGEREQUEST.JSP
33630956	ENTEROTP.JSP USED IN PASSWORD FLOW DOES NOT HANDLE FRENCH LOCALE

Table 1-13 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220404

Base Bug Number	Description of the Problem
33690341	INVALID INPUT WITH SPECIAL CHAR ON CLIENT_ID & CLIENT NAME You can use this feature by adding the following Java property in `setDomainEnv.sh`: `-Doracle.oam.oauth.allow.all.char=true`
33654883	OAM 12CP4:IN AUTHORIZATION POLICIES SESSION CUSTOME OR DYNAMIC ATTRIBUTES CONFIGURED FOR HEADER/COOKIES NOT RETRIEVED IN RESPONSE
33585810	UNSOLICITED LOGIN FAILS WITH OCT CPU PATCH USING CUSTOM PLUGIN.
33560440	PERFORMANCE ISSUE RELATED AM_SESSION TABLE DESPITE ENH 29337161 APPLY
33521038	OAM 12CPS4 BP8 EMAIL CLAIMS SCOPE IS MISSING IN THE ID TOKEN
33604911	NULLPOINTEREXCEPTION ON REST QUERY ON ../TRUSTEDPARTNERS/SP ENDPOINT
33554950	OCTOBER 2021 CPU PATCH BREAKS FEDERATION LOGIN If OAM is used as a federation proxy, add below System property in `setDomainEnv.sh` : `-Doam.federationProxyEnabled=true`
33527784	OIDC + WEBGATE APPS FAILING IN CLONE DC\S AFTER UPGRADE TO 12.2.1.4
33392806	FEDERATION: ATTRIBUTES CONFIGURED IN SP MAPPING PROFILE EMPTY IN SAMLRESPONSE

Note:

This is relevant only when different user identity stores are used for the OAuth identity domain and Authentication Policy for the OAuth consent resource. The following system property must be set in `setDomainEnv.sh` to enable this fix:
`-Doam.sessionRetrievalWithId=true`

Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

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

Table 1-14 Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Base Bug Number	Description of the Problem
33533200	AUTHZ CALL FAILS WHEN RDN HAS SPECIAL CHARACTER **Note:** This bug is dependent on libovd patch 33638694.
33518405	Fix for Bug 33518405
33474333	MDC: FAILURE TO GET ACCESS TOKEN FROM AUTHZ CODE IN LOCAL DC **Note:** This is relevant only when different user identity stores are used for the OAuth identity domain and Authentication Policy for the OAuth consent resource. The following system property must be set in `setDomainEnv.sh` to enable this fix: - `Doam.sessionRetrievalWithId=true`
33368662	HTTPTOKENEXTRACTOR PLUGIN DOES NOT PUT HEADER NAME IN THE CREDENTIAL PARAMETER **Note:** Headers must be comma separated if more than one header is configured in `KEY_HEADER_PROPERTY` for `HTTPTOKENEXTRACTOR` plugin in the authentication module.
32923468	MDC: ADAPTIVE AUTHENTICATION MODULE

Table 1-14 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.220113

Base Bug Number	Description of the Problem
33389214	INVOKING THE OAM SESSION REST API GET BAD REQUEST ERROR.
33358965	CHANGE PASSWORD RULES APPEAR TO BE URL ENCODED ON THE /OTPFP/USERSELECT PAGE
33391677	FEDERATED USER HAVING \ IS SENDING \5C\ TO LIBOVD WITH FILTERESCAPE VALUE TRUE **Note:** This bug is dependent on libovd patch 33638694.
33142450	USER STILL RETURNED TO THE URL EVEN WITH RETURNURLVALIDATIONENABLED
33069979	TAP INTEGRATION BETWEEN 12CPS4 OAM AND 11GR2PS3 OAAM IS NOT WORKING **Note:** The following Java parameter must be set to `true` in `setDomainEnv.sh` to enable this feature: `-Doam.enable.legacy.client=true` By default, it is `false`.
33242499	STRESS:FA:ATK:FMW12C: LOGON STORM TEST IS FAILING WITH 500 CLIENTS
33275487	STRESS:FA:ATK:FMW12C: CONCURRENTMODIFICATIONEXCEPTION SEEN IN OAM LOGS WHEN DIAGNOSTIC LOGGING ENABLED
33109073	OAMREAUTHENTICATE WORKS ONLY FIRST TIME

Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

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

Table 1-15 Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
33192650	"SYSTEM ERROR" ON THE CLONE DATA CENTER WITH OAM 12.2.1.4.210408 (BP06)
33214625	REDIRECT URI VALIDATION DOESN'T SUPPORT QUERY PARAMS, FRAGMENTS, ETC
33273701	CREATE CLIENT ARTIFACT ENDPOINT DOESN'T SUPPORT THE MEDIA TYPES MENTIONED IN REST DOCUMENTATION
33273732	NO GET API ON CLIENT/TRUST ARTIFACTS (ONLY POST OR DELETE AVAILABLE)
33273741	ISSUES WITH DISCOVERY END-POINT
33273750	TOKEN INTROSPECTION ENDPOINT DOESN'T CONFORM TO SPECIFICATIONS
32958613	JWT TOKEN CONTAINE GROUP IN INCORRECT FORMAT
33273674	MUTUAL TLS FOR OAUTH CLIENT AUTHENTICATION
33273579	CLI AND REST COMMANDS TO EASE SFA TOTP SETUP IN OAM
31517286	Fix for Bug 31517286
32102796	ALLOW SENDING ADDITIONAL CUSTOM CLAIMS INSIDE OIDC ID TOKEN WHEN OAM IS IDP
32201831	ABILITY TO PULL EMAIL VERIFIED CLAIM IN ID TOKEN FROM LDAP
30045443	OAM OAUTH: FEATURE TO GENERATE OAUTH TOKEN WITH TPC
33098826	UNSOLICITED LOGIN FLOW BREAKS WITH PASSWORD POLICY WITH SFA FLOW
33055065	FEDERATION NOT WORKING AFTER ACCESSING OAM PROTECTED PAGE
31431111	ON THE LOGOUT CONSENT PAGE, WORDING SHOW "SIGN IN" INSTEAD OF "SIGN OUT"
32761540	STRESS:FA:ATK:FTS ON AM_AUDIT_RECORD FROM SQL 8RWNP1YMTMWWB
33117541	NON-PROXY HOST EXCEPTIONS DO NOT WORK
33139217	OAM_ADMIN FAILS TO START AFTER APPLYING 12.2.1.4 APRIL/JULY 2021 BP
32920684	IMPORTPOLICYDELTA FAILS TO IMPORT ADVANCED AUTHENTICATION RULES
33084122	12C 21.07 EVNI: "ACCESS SERVER HAS RETURNED A FATAL ERROR WITH NO DETAILED INFORMATION" ERRORS IN OHS LOGS (WEBGATE)
33074398	ISSUE WITH APNS PATCH 32625905: SOUND MISSING
33010382	SPECIAL CHAR ON PASSWORD FIXED IN 29771448 & 31555915 NO LONGER WORK AFTER BP06
32807465	DELETING IDENTITY PROVIDER CANNOT REPLICATE TO CLONE SERVER FROM MASTER

Table 1-15 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32704611	NOT ABLE TO CREATE OAUTH CLIENT IF ATTRIBUTE VALUE CONTAINS BACKSLASH **Note:** To enable the backslash (\) attribute value, edit `setDomainEnv.sh` and add the following system property: `-Doracle.oam.oauth.allow.backslash=true` The default value is `true`.
32909931	OAM NOT SETTING AUTHN RESPONSE HEADERS AFTER APPLY 12.2.1.4.210408
32543656	OAM 11G (SP) SHOULD END THE LOCAL SESSION WHEN RECEIVING SOAP LOGOUT REQUEST
32482754	INCREASE OAUTH ACCESS TOKEN MAXIMUM SIZE TO MORE THAN 5000 CHARACTERS
32879893	INTERMITTENT ERRORS IN OAM CONSOLE PREVENT VIEWING & UPDATING POLICY OBJECTS
32976735	EBS APPSLOGIN FAILS WHEN USING OAM WITH OUD AS BACKEND LDAP ON AIX WITH TLS 1.2 ONLY
32568653	12 VERSION : ACCESSSERVERCONFIGPROXY PORT CHANGING 5576 TO 5575 RESTARTADMIN **Note:** To trigger the topology update, set the following system property in `setDomainEnv.sh`: `-Doam.t2p.enableTopologyUpdate=true`
32953208	OAM OPENID CONNECT LOGOUT DOES NOT FORWARD STATE PARAMETER TO POST_LOGOUT_REDIRE
32933119	API /OAUTH2/REST/SECURITY DO NOT WORKING ERROR 406

Table 1-15 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
27582324	POST DATA RESTORATION FAILS WHEN OBRAR.CGI USES GET METHOD TO RETRIEVE DATA.
31843528	ASSERTION HAS AN ADVICE ELEMENT THAT CONTAINS AN ENCRYPTED FIELD THAT FAILS OAM
32828842	OIDC-PIREAN INTEGRATION - NOT A VALID JWT TOKEN
32826737	TEST CONNECTION FOR LDAP IN OAM CONSOLE FAILS FOR TLS 1.2 ON IBM AIX **Note:** In IBM AIX OS 7.1 or 7.2 having OAM and OID set on TLSv1.2, ensure that you set the following OAM system property in `setDomainEnv.sh`: – `Djdk.tls.client.protocols=TLSv1.2` and restart the OAM Admin Server.
32734517	NOT ABLE TO UPDATE THE AUTHNSCHEMELEVEL FROM 5 TO 2 FOR X509 USING CURL
31859438	12C :OAUTH CLIENT : UPDATE : REDIRECT URI : SUPPORT FOR HTTP PATCH REQUEST
32655233	LIBOVD 12C SPECIAL CHARACTER IN USERNAME FAILS TO LOCATE USER IN LDAP **Note:** This bug is dependent on libovd patch 32305678.
32701831	REDIRECT LOOP USING INITIAL_COMMAND=NONE AFTER APPLICATION DOMAIN IDLE TIMEOUT
32501273	REMOTE IP NOT APPEAR INTO AUDIT DATABASE FOR OAUTH AUTHORIZATION
32653281	"FAILED TO INIT CONTEXT PATH:/IDAAS/AM/ESSO" ERROR IN ADMIN SERVER STARTUP LOGS

Table 1-15 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210920

Base Bug Number	Description of the Problem
32561825	AUTHMON - OAM AUTHMON (OAM-MON.SH) - NEED TO IMPLEMENT LOGOUT SO SESSIONS DO NOT BUILD UP.
32650194	FIX FOR BUG 32487114 IS NOT WORKING IN OAM REL13 PATCH 32628242
27584970	CAPACITY CONSTRAINT IN WEBLOGIC-APPLICATION.XML CAUSING PERFORMANCE IMPACT

Note:

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

```
<case
uuid="a46c2914-30
c7-4b20-8862-
c244fd0d74d5">
    <request
code="logout"/>

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

<comment></
comment>

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

<content></
content>
        </
response>
</case>
```

Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

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

Table 1-16 Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

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

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

Table 1-16 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210607

Base Bug Number	Description of the Problem

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

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

Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

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

Table 1-17 Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

Base Bug Number	Description of the Problem
29244150	SSO BETWEEN TUNNELED DCC AND PLAIN DCC IS BROKEN WHEN APPLIED OAM BP'S 14,15 OR 16
27441865	CLIENTSSLKEYSTOREPWD, CLIENTSSLTRUSTSTOREPWD NOT PROPERLY WRITTEN IN OAM-CONFIG
28728420	OAM-OIM FIRSTLOGIN PAGE IS BLANK, BACKURL CONTAIN HOST IDENTIFIER
32612533	OAM 12CPS4 SSO BETWEEN FED SP1 AND SP2 PARTNER PROTECTED RESOURCE IS FAILING WITH APRIL BP 32525944
32153972	SIGNATURE VALIDATION FAILED OPENIDCONNECTPLUGIN CONFIGURATION
32392692	ORACLE CLOUD MCS_LOGIN_324.PNG NOT BEING USED AND APPEARS IN LOGIN PAGES
32632139	OAM 12CPS3 FIX FOR BUG 32055280 IS FAILING
32433361	ASDK INITIALIZATION FAILING
32477536	ASDK FAILED TO INITIALIZE IF COMPATIBILITYMODE IS OAM_12C
18957556	NOT GETTING P_ERROR_CODE=OAM-3 IN DIAGNOSTIC LOGS WHEN OID IS DOWN
29725629	Fix for Bug 29725629
31386392	NOTSTRESS:FA:ATK:ORACLE.OAM.BINDING ERRORS IN IDM WLS_OAM1 LOGS
27962394	USER WAS APPENDED WITH POD NAME
31994408	OAM LOGIN PAGES CHANGES TO ADAPT TO REDWOOD UI STYLE
30155115	OIFAUTOMATION.PL ENABLEOIF FAILURE - WRONG DB SCHEMA PASSWORD USAGE
31430985	IN THE INITIAL SIGN ON PAGE, THE TEXTBOX "USER ID" AND "PASSWORD" FIELD DOES NOT HAVE A LABEL
32430636	12C: 500 INTERNAL SERVER ERROR IN FAHOME PAGE
32394988	FOREGROUND AND BACKGROUND COLOURS DOES'T MEETS WCAG 2 AA CONTRAST RATIO THRESHOLDS
32487114	WCAG 2.0-2.4.1: PAGE MUST HAVE MEANS TO BYPASS REPEATED BLOCKS.
32451171	KM AUTOMATION : ADD AUTOMATION SCRIPT FOR CONFIG CHANGES IN BUG# 32380923
27481308	ER: OAM OAUTH PKCE (RFC 7636) SUPPORT
32507312	ISSUE ACCESSING /OAMFED/USER/SLOOAM11G?ID=OAM11G&TYPE=3
29337161	12C UPDATES THE AM_SESSION TABLE IN THE DB FOR EVERY AUTHZ REQUEST

Table 1-17 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.210408

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

Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

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

Table 1-18 Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

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

Table 1-18 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

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

Table 1-18 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

Base Bug Number	Description of the Problem
31641787	OUD ATTRIBUTE RESETPWD:TRUE CAUSES AUTHN FAILURE FOR USERAUTHENTICATIONPLUGIN **Note:** You can allow authentication for Oracle Unified Directory password policy attribute `RESETPWD=true` by adding the following attribute to the `oam-config.xml` file under the configured user identity store: `<Setting Name="checkPwdPolicyWarning" Type="xsd:boolean">false</Setting>`
31650595	UNABLE TO START INTERNAL STAGE PRIMARY
31428183	WEBGATE PROFILE GET CORRUPTED IF ADD PRIMARY/SECONDARY SERVER WITH N+2 INDEX USING WEBGATE TEMPLATE.
31039212	GLOBAL LOGOUT NOT CLEARING SESSION
31857424	Fix for Bug 31857424
31744937	REST API:OTP:CREATEOTP & VALIDATEOTP FLOWS NEEDS TO BE FIXED
29154366	OAM-OSB INTEGRATION USING OAUTH2 NOT WORKING
31638527	NULL POINTER EXCEPTION WITH PASSWORD MANAGEMENT DISABLED
28562000	PREAUTHENTICATION RULE TO DENY ACCESS DISPLAYS OPERATION ERROR
31728627	CONCURRENCY ISSUES IN SecurityConfig/TrustedInputs INITIALIZATION.
31595758	SOME SAML ATTRIBUTES GET MAPPED TO WRONG AVALUES AFTER SAML RESPONSE WITH OAM 12C
31741829	STUCK THREADS IN ORACLE.SECURITY.FED.SECURITY.UTIL.CERTRETRIEVALUTILS.GETSIGNINGCERT IN SAML LOGIN FLOWS

Table 1-18 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.201201

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

Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

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

Table 1-19 Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
31666896	OAM AUTHENTICATION REST API
31516886	USERS CAN'T VIEW APPLICATION DOMAINS IF OAMCONSOLE IS PROTECTED BY WEBGATE
31753451	ERROR WHEN RUNNING WLST COMMAND SETSPPARTNERATTRIBUTEVALUEFILTER
28296759	FORCE PASSWORD RESET NOT WORKING WITH BASIC METHOD AND FORM CACHETYPE
25853168	AFTER UPGRADE TO R12 ONE/FEW CURL COMMAND FOR FEDERATION IS NOT WORKING
29058490	OAM OIM INTEGRATION - LOGIN LOOP AFTER THE USER IS UNLOCKED
27566767	ENH 27566767 - BACKWARD COMPATIBILITY : WITH OAM AS IDP PROVIDE ATTRIBUTE MAPPINGS AND FILTERS IN OAM 12C LIKE OIF 11G
31111719	12CPS4:BP02:ERROR POP UPS ON OAMCONSOLE UI
31427426	SHOWING INVALID PARAMETERS WHILE UPDATING PRIMARY/ SECONDARY SERVER PARAMETERS.
30589288	OIDC SOCIAL LOGIN FAILS DUE TO BLOCKURLS SECURITY CONFIGURATION
30804658	WIN2012R2: NEED TO HANDLE SQL VIOLATION AT ADMIN SERVER BOOTSTRAP
31196076	IPFPSWD.JSP IS THROWING SYSTEM ERROR

Table 1-19 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
26565827	AWS ROLE MAPPING ATTRIBUTE SUPPORT
31186283	ESCAPE CHARACTERS ADDED WHEN CREATING OAUTH TOKEN
31555915	SPECIAL CHARS ON PASSWORD DOES NOT AUTHENTICATE AFTER UPGRADE TO 12.2.1.4
28040138	ORACLE ACCESS MANAGER OPERATION ERROR WHEN AUTHZ POLICY SUCCESSURL IS CONFIGURED
31501282	OAM SYSTEM ERROR ON FORCE PASSWORD CHANGE AFTER APPLYING 12.2.1.3.191201 (BP07)
23096690	PUMA - PERFORMANCE ISSUES SEEN IN APS SYNC-ADD/UPDATE WEBGATE
31038100	ADVANCED RULE PARSING RETURNS UNEXPECTED RESULT FOR ATTRIBUTE EVALUATION

Note:

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

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

```
EXTRA_JAVA_PROPERTIES="-
Doam.rule.userAttr=<userAttr1>::<
attrValue>,
<userAttr2>::<attrValue>
${EXTRA_JAVA_PROPERTIES}"

export EXTRA_JAVA_PROPERTIES
```

For example:

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

export EXTRA_JAVA_PROPERTIES
```

31289851	OAUTH/OIDC APPROVAL WORKS WHEN NO SESSION FOUND
31337500	OAM MT STUCK THREADS AND HIGH CPU - UIDMX0113
30235925	OAM SESSION SUPPORTS ONLY 40 STRING TYPE PROPERTIES
31068961	ORA-01461: CAN BIND A LONG VALUE ONLY FOR INSERT INTO A LONG COLUMN

Table 1-19 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200909

Base Bug Number	Description of the Problem
28855754	12.2.1.3 OUD PASSWORD POLICY ATTRIBUTE RESETPWD SET TO TRUE CAUSES AUTHN FAILURE
29120924	AMRUNTIMEEXCEPTION:INVALID SETTINGS FOR FORWARD WHEN INTEGRATING DUO PLUGIN
27963081	LDAP RESPONSE READ TIMED OUT - ON IDSTORE CREATION, IF "SEARCH BASE" IS "HUGE"

Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

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

Table 1-20 Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
31065568	INTERIM FIX : NEED TO MAKE SURE ALL COOKIES ISSUE BY OAM11G & 12C CONTAIN SAMESITE=NONE
31465732	OAMS.OAM_RESOURCE_URL WARNING MESSAGES STILL DISPLAY IN OAM LOGS WITH FIX 30053037
30053037	OAMS.OAM_RESOURCE_URL WARNING MESSAGES IN OAM LOGS
31510690	PASSWORDRESETREQUESTS REST END POINT THROWS INTERNAL SERVER ERROR.
31508059	INVALID SESSION CONTROL PARAMETERS
30622957	X509 RFC (SECURITY): OAM AUTHN WITH EXTENDEDKEYUSAGE
31366419	UPDATE VALIDATE ENDPOINT TO WORK WITH POST
31413189	MODIFY MDC SESSION CONTROL API FAILES WITH MDC NOT ENABLED ERROR
31419785	THE OAMCUSTOMPAGES.WAR IS NOT DEPLOYABLE.

Table 1-20 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
30953737	WLS ADMIN SERVER LOG FILE AFTER APPLYING AN OAM BUNDLE PATCH THE FOLLOWING WARNING IS NOW SEEN - SOFTLOCK IS ENABLED BUT IS NOT RECOMMENDED SETTING IN PRODUCTION ENVIRONMENT **Note:** To understand how to run the script for disabling/enabling softlock, refer to **readme.txt** in the following directory: `$MW_HOME/idm/oam/server/wlst/scripts/utilities/`
31110638	OAM 12.2.1.4 APR20 BP - IMPORTPOLICY WLST FUNCTION TAKING VERY LONG TIME TO IMPORT POLICIES
29883498	OAM/MDC ISSUE: INVALID SIMPLE MODE ARTIFACTS
30669352	AUTHORIZATION RESPONSE NOT RETURNED FOR AUTHORIZATION FAILURE
30748479	CLIENT IP NOT CAPTURED IN AUDIT.LOG FOR REST CALLS
30406633	GETTING NOT_FOUND WHILE FETCHING ATTRIBUTE FOR SAML RESPONSE HEADER
30762860	Fix for Bug 30762860
31000954	12CPS4 : FEDERATION USES LOCAL IN MEMORY STORE
30120631	SMS OTP PAGE REFRESH
30911495	TWO FACTOR AUTHENTICATION ENTRY TEXTBOX DOES NOT GAIN FOCUS IF THERE IS ONLY ONE OPTION FOR 2ND FACTOR AUTHENTICATION
30628496	UNABLE TO MODIFY PRIMARY/SECONDARY SERVER DATA USING CREATEWEBGATETEMPLATE SYNTAX
30831364	HTTP 405 ON WNA CRED COLLECT ENDPOINT EVEN THOUGH ENDPOINT NOT IN BLOCKURLS LIST

Table 1-20 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200629

Base Bug Number	Description of the Problem
30771422	ADVANCED RULE PARSING FAILS FOR MAP PARAMETERS (USER.USERMAP, REQUEST.REQUESTMAP **Note:** See also the note Oracle Access Manager (OAM) "Invalid rule condition" Error On Advanced Rules (Doc ID 2664614.1) at https://support.oracle.com.
30882267	OAM CUSTOM PAGES LOGIN.JSP IS NOT WORKING IN OAM 12.2.1.4
28108712	MODIFY MDC SESSION CONTROL REST API FAILS
29715441	OAM: USERINFO REST CALL DOES NOT RETURN CORRECT VALUE OF TELEPHONENUMBER FOR LDAP PROVIDER OUD
30832165	FEDERATION: FEDSTS-10202: COULD NOT RETRIEVE MDC DATA FROM CLUSTER
30793308	OAM IDP: SYSTEM ERRORS SEEN INTERMITTENTLY DURING FEDERATION LOGOUT
30355996	OAM SESSION API RETURN HTTP 500 ERROR WITH CEST TIMEZONE

Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

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

Table 1-21 Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Base Bug Number	Description of the Problem
30805180	OAM Snapshot Tool
30805164	OAUTH CONSENT LIFECYCLE MANAGMENT AND MDC SUPPORT
30805154	OAUTH JUST IN TIME /JIT PROVISIONING

Table 1-21 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Base Bug Number	Description of the Problem
30820170	AUTHORIZATION ERROR WITH USER MEMBER LARGE NUMBER OF GROUP
30792754	MDC ENV. CUSTOM ATTRIBUTES ARE NOT INCLUDED IN ACCESS TOKEN
21391069	NEED TO LOG AUTHENTICATION FAILURE AUDIT LOG FROM CUSTOM PLUGIN
29717855	SAML LOGOUT NOT WORKING IF OLD FED SESSIONS EXIST IN DB
29240849	NEED TO LOG ADDITIONAL AUTHENTICATION FAILURE FOR AUDIT LOG FROM CUSTOM PLUGIN
30634571	12C OAUTH AUDIT RECORDS RETURN NULL VALUES FOR OAUTHTOKENVALIDATE EVENTS
30571576	K8S : OAM_ADMIN AND OAM_SERVER APPLICATION DEPLOYMENT FAILED K8S CLUSTER
29783271	UPDATE OF OUD DETAILS DELETES CONFIG ATTRIBUTE ENTRY ADDED FROM OAM-CONFIG.XML
29885236	ENABLED MULTIVALUEGROUPS SP USE $USER.GROUPS TWICE IN A FED SP ATTRIBUTE PROFILE
30134427	Fix for Bug 30134427
30169956	OAUTH PASSWORD GRANT TYPE CAN ONLY USE NON-PLUGIN LDAP MODULE FOR AUTHENTICATION
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 the managed server using the Webgate's user-defined parameter `tunnelingDCCReadTimeout`. Specify the `tunnelingDCCReadTimeout` in seconds, for example, `tunnelingDCCReadTimeout=30`. **Note:** When specifying `tunnelingDCCReadTimeout`, you must also increase `aaaTimeoutThreshold` accordingly.
30460435	DCC TUNNELING WHITELIST CAN NOT BE DISABLED USING ENABLEWHITELISTVALIDATIONDCCTUNNELING CONFIG

Table 1-21 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.200327

Base Bug Number	Description of the Problem
30426370	OAM 12.2.1.4:DOWNLOADACCESSARTIFACTS: SEVERE:REQUEST TO PROCESS ARTIFACTS FAILED
30468914	OAM DOES NOT SUPPORT HOLDER OF KEY PROFILE.
30069618	OAMAGENT-02077: AUTHN TOKEN IS EITHER NULL OR INVALID

Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

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

Table 1-22 Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

Base Bug Number	Description of the Problem
26679791	FIX FOR BUG 25898731 IS FAILING IN OAM 11.1.2.3.171017BP 26540179
30389257	TWO FACTOR AUTHENTICATION ENTRY TEXTBOX DOES NOT GAIN FOCUS
30311080	OIGOAMINTEGRATION.SH - CONFIGURESSOINTEGRATION THROWS UNMARSHAL EXCEPTION IN FRESH 12CPS4 ENV
30156706	OAM ADMIN SERVER START FAILS DUE TO FAIL TO CREATE OAM-CONFIG.XML FROM DBSTORE
29771448	% CHAR IN PASSWORD USED TO GENERATE OAUTH ACCESS TOKEN IS TRANSLATED TO ASCII
30144617	ISSUE ON CHANGE IN BEHAVIOR IN RETURNING ERRORCODE AFTER APPLYING PATCH 29918603
29482858	OAM 11G ASDK INTERMITTENTLY THROWING ERROR WHILE CREATING OBSSOCOOKIE
29541818	ER TO ADDRESSING ADDITIONAL USE CASES OF OAUTH AND JSON IN OAM 12C
29837657	OAM DOES SUBTREE SEARCH TO VALIDATE IDSTORE CREATION
29290091	WRONG SELECT IN ADMIN STARTUP LOGS
30156607	DIAG: ADD MORE LOGS IN AMKEYSTORE VALIDATION FLOW TO IDENTIFY CONFIG THAT CAUSES TO FAIL TO START ADMIN SERVER
30243111	DIAG: REQUIRE LOGS IN DEFAULT KEYSTORE BOOTSTRAPPING FLOW TO IDENTIFY CONFIG MISSING/ CORRUPTION ISSUE
30180492	OCI FEDERATION WITH ORACLE ACCESS MANAGER IS NOT WORKING AS EXPECTED
30363797	OAM11GR2PS3 : WNA_DCC MODULE IS FAILING WITH SECURITY BUG FIX :25963019

Table 1-22 (Cont.) Resolved Issues in OAM Bundle Patch 12.2.1.4.191223

Base Bug Number	Description of the Problem
29649734	12.2.1.3.180904 (BP04) ACCESS SERVER RETURNS JSON KEY AND NOT P7B LIKE DOCUMENT
30062772	FEDERATION BP18 CAUSES LOGOUT END_URL TO BE CONVERTED TO LOWER CASE IN FED LOGOU
30176378	ERRORS IN OAM SERVER LOGS AFTER RUNNING WLST COMMAND DISABLESKIPAUTHNRULEEVAL()
30267123	UNABLE TO LOGIN FROM MULTIPLE TABS AFTER LOGGING IN FROM A TAB.

Known Issues and Workarounds

For known issues and workarounds refer to:

- My Oracle Support Document 2602696.1 at https://support.oracle.com
- The workaround for Bug 34636811 can be found at My Oracle Support Document 2901185.1 at https://support.oracle.com

Oracle Fusion Middleware Oracle Access Management Bundle Patch Readme, OAM Bundle Patch 12.2.1.4.250428 Generic for all Server Platforms
G29738-01