ORACLE

Public

EPM Cloud Deep Dive

Application and Infrastructure Best Practices

Vinay Gupta

November, 2023

Safe Harbor

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at http://www.oracle.com/investor. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.

Agenda

- OCI Migration
- New Features in OCI
- User Management and SSO
- Security Best Practices
- Daily Maintenance and Backup
- Activity Report
- EPM Cloud Operations Guide and Application Design Best Practices

EPM Cloud Migration to OCI

- All EPM Cloud Commercial environments will be migrated to OCI by the end of November 2023.
  - All Classic Commercial environments will be terminated, starting December 1, 2023.
- US-Gov and UK-Gov environments will be migrated in 2024.

Why Migrate to OCI?

- As the foundation of Oracle's second-generation cloud, OCI is purpose-built, best-in-class platform for running enterprise applications.
- OCI is engineered from the ground up to run mission-critical databases, workloads, and applications while providing end-to-end security.
- Oracle's data centers around the globe are standardizing on the OCI architecture which delivers greater performance and reliability.
- Many features of EPM Cloud are available only in OCI.

Features Available Only in OCI – 1 of 4

Feature	Description
Oracle Cloud Identity Console or Oracle Cloud Console (IAM)	Perform user and security management tasks such as creating users, removing users, assigning and unassigning roles, and setting up Single Sign-On (SSO).
New audit reports and logs	Role Assignment Audit Report and Invalid Audit Report are available through EPM Automate and REST APIs.
	Application Role Privileges Report, Successful Login Attempts Report, Unsuccessful Login Attempts Report, and Dormant Users Report are available from Oracle Cloud Identity Console, Oracle Cloud Console (IAM), and through Oracle Cloud Identity Service REST APIs.
	Audit log containing information on successful and failed logins, and user management actions (user creation, update, and deletion) is available from Oracle Cloud Identity Console, Oracle Cloud Console (IAM), and through Oracle Cloud Identity Service REST APIs.
OAuth 2 Support for REST API, EPM Automate, and EPM Integration Agent	Use OAuth 2 access tokens to make REST API calls to EPM Cloud and to use EPM Automate and EPM Integration Agent to avoid the use of passwords.
Support of multiple SAML 2.0-compliant identity providers for a domain	You can configure SSO for a domain with multiple SAML 2.0-compliant identity providers simultaneously.
Support of Identity Provider Groups	You can add individual users to an Identity Cloud Service (IDCS) group and then assign predefined roles to the group. Since IDCS groups can be synced with Identity Provider groups (such as Azure AD) groups), you can even add individual users to Identity Provider groups and assign the predefined roles to these groups in Oracle Cloud Identity Console or Oracle Cloud Console (IAM). See Using Identity Cloud Service Groups to Assign Predefined Roles to Users in Oracle Cloud Identity Console (for OCI (Gen 2) only)

Features Available Only in OCI – 2 of 4

Synchronize IDCS users and groups across identity domains	You can use System for Cross-domain Identity Management (SCIM) to enable automatic provisioning of users and groups between identity domains supported on IDCS. See Using SCIM to Synchronize Users and Groups on Oracle Identity Cloud (for OCI (Gen 2) Only)
Ability to rename the instance	You can change the instance name and, consequently, the URLs of your environments using My Services (OCI). See Rename an OCI (Gen 2) EPM Cloud Instance.
Private access to EPM Cloud	If you have an OCI IaaS subscription in the same data center as your EPM Cloud environments, you can use the Service Gateway Service to avoid having traffic go over internet. See Use of Dedicated VPN Connection to Restrict Access in *Oracle Enterprise Performance Management Cloud Operations Guide*.
Change Password Policy	You can set your own password policy. For details, see Manage Oracle Identity Cloud Service Password Policies in *Administering Oracle Identity Cloud Service*.
Restrict user access	You can deactivate environments so that user cannot sign in to them. For details, see Deactivate Access to OCI (Gen 2) Environments. You can also configure a custom sign-on policy to restrict access to users with specific predefined roles. For details see Sign-On Policies to Restrict Access to OCI (Gen 2) Environments
Maximum session duration	You can set the maximum session duration in Oracle Cloud Identity Console or Oracle Cloud Console (IAM) to log out the user, even if the user is actively using the environment. See Maximum Session Duration in OCI (Gen 2) Environments
Virus scan on uploaded files	OCI (Gen 2) environments provide an option to enable the virus scan on uploaded files. When this option is enabled, each uploaded file is scanned for virus. If a virus is detected, the file is not uploaded.

Features Available Only in OCI – 3 of 4

Block connections from specific countries	You can request Oracle to block all connections originating from specific countries. For details, see Requesting the Blocking of Connections Originating in Specific Countries to OCI (Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide*
Allow connections from specific countries only	You can request Oracle to allow connections originating from specific countries only and block connections from other countries. For details, see Requesting to Allow Only Connections Originating in Specific Countries to OCI (Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide*
Database encryption using AES-256	OCI (Gen 2) uses AES-256 to encrypt the master key as well as tablespace to satisfy the requirement to encrypt data at rest in relational database. The master key is rotated regularly.
OCI Block Volume Encryption	To encrypt data at rest, OCI (Gen 2) uses Block Volume Encryption using AES-256 to encrypt file system data including Oracle Essbase data.
Self-service option to list and restore available backup maintenance snapshots	Artifact snapshots resulting from daily maintenance of OCI (Gen 2) environments are archived to Oracle Object Storage daily. Production environment backups are retained for 60 days while test environment backups are retained for 30 days. OCI (Gen 2) environments support self-service operations using the listBackups and the restoreBackup EPM Automate commands to check for and copy available backup snapshots from Object Storage to your environment.
Encryption Keys stored in FIPS 140-2 compliant Hardware Security Module (HSM)	In OCI (Gen 2) environments, all encryption master keys including the following are stored in FIPS 140-2 compliant HSM: • Transparent Data Encryption (TDE) master key for database encryption • Block Volume Encryption master key for file system encryption • Object Storage Encryption master key for encryption of artifact snapshots

Features Available Only in OCI – 4 of 4

Web Application Firewall (WAF) support	In OCI (Gen 2) environments, Web Application Firewall (WAF) is available out-of-the-box and protects EPM Cloud from many application layer attacks.
DKIM (DomainKeys Identified Mail) support	EPM Cloud on OCI (Gen 2) environments supports DKIM for outgoing messages. See DKIM Support for EPM Cloud OCI (Gen 2) Environments
Customization of Sign-in Page	You can customize the Oracle Identity Cloud Service sign-in page using the Authentication REST API. See Customize the Oracle Identity Cloud Service Sign-In Page Using the Authentication API for instructions.
Customization of Notifications	You can modify the notification templates for the email notifications Identity Cloud Service sends for activities, such as user addition, role assignment, and password expiry. You can select the notification language, the activities for which notifications are to be sent, the email sender, subject, and body.

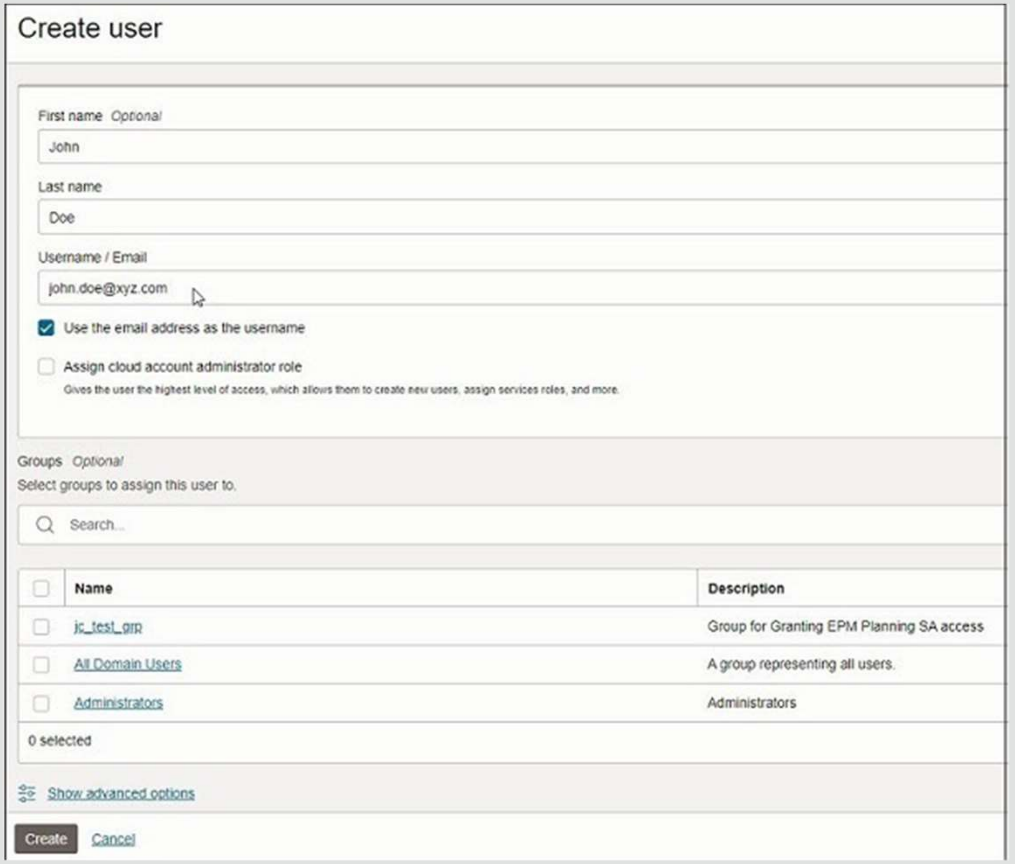
Renaming EPM Cloud Environment

- Rename the service name part of the EPM Cloud environment to make it more user-friendly.
  - The new service name is part of the URL. So, all scripts, bookmarks, Smart View connections, etc. need to be updated to account for the new URL.
  - Renaming tenant/account name available in future.

Steps: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/1_about_epm_cloud_change_instance_name.html

User Creation

- **Oracle Cloud Console**
- **EPM Automate:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_add_users.html
- **EPM Cloud REST API:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_add_user_to_identity_domain_v2.html
- **IDCS REST API:** https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/op-admin-v1-users-post.html

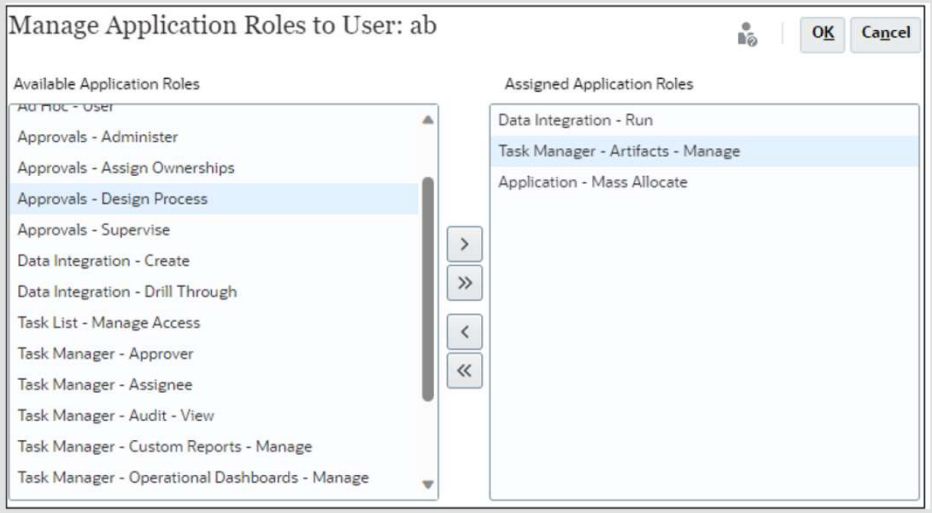


Predefined Role Assignment

- **Oracle Cloud Console**
- **EPM Automate:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_assign_roles.html
- **EPM Cloud REST API:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_assign_role_v2.html
- **IDCS REST API:** https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/api-apps-app-roles.html

Application Role Assignment

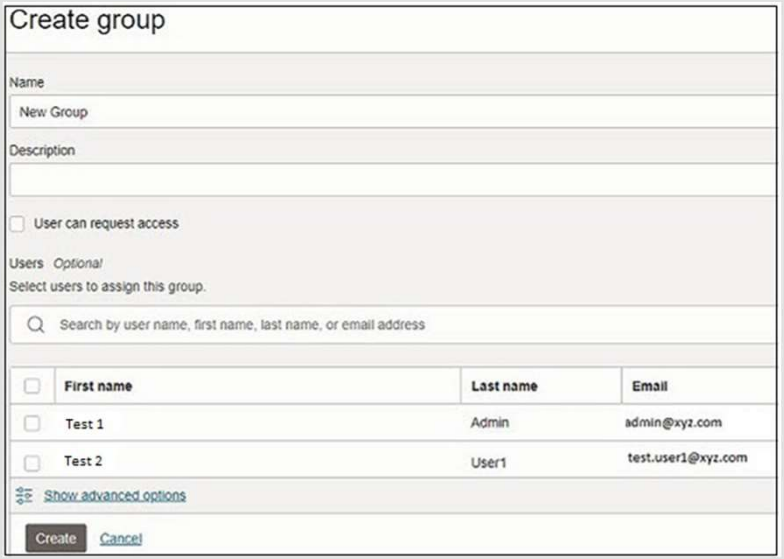
- **Access Control**
- **EPM Automate:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_assign_roles.html
- **EPM Cloud REST API:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_assign_role_v2.html

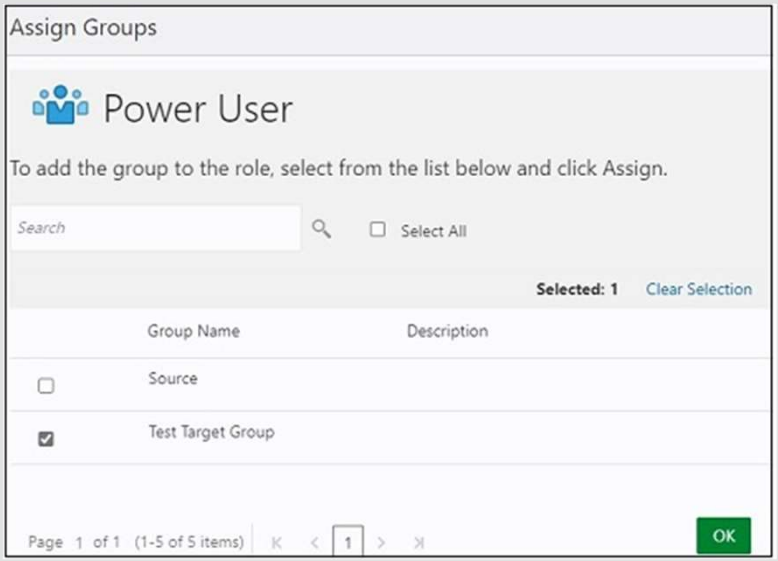


IDCS Group Support

Ability to use IDCS groups to assign predefined roles

- All users in an IDCS group inherit the roles assigned to the group.
- IDCS groups can be synced with Azure AD groups, MSAD groups, etc.

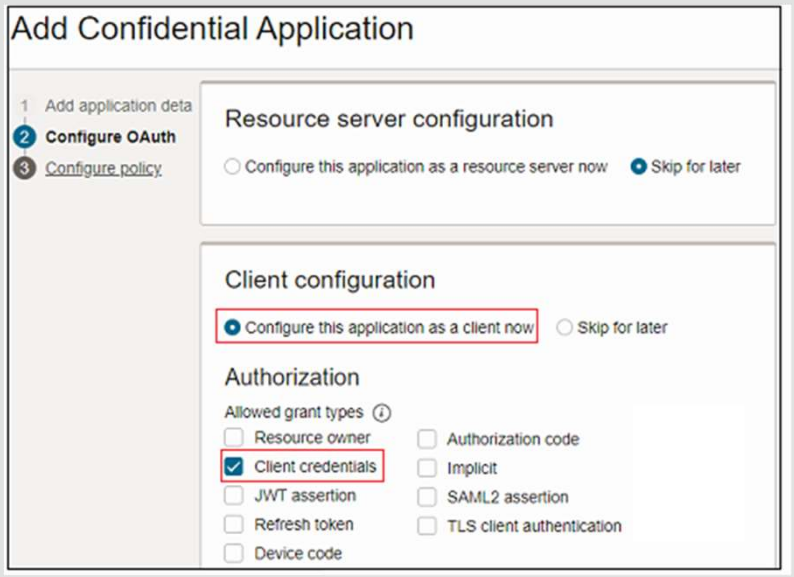


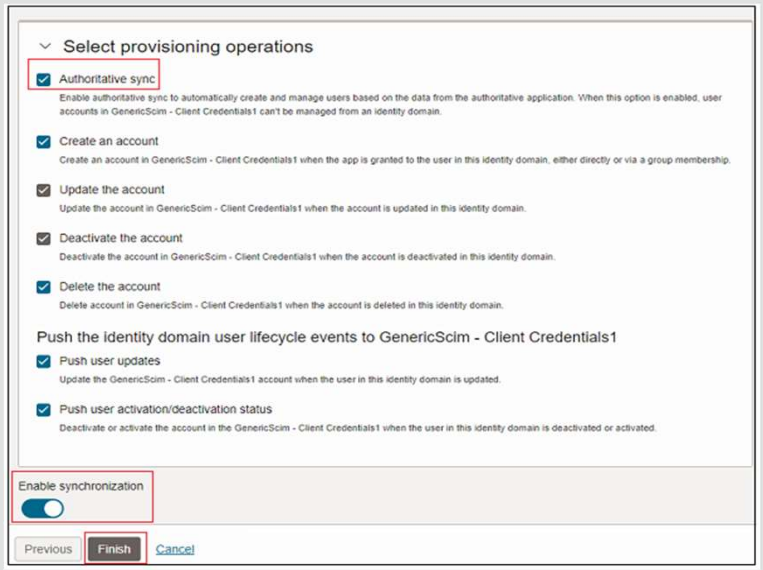


SCIM (System for Cross-Domain Identity Management) Support

Ability to sync users and groups from other Identity Management products (e.g., another IDCS, Azure AD, etc.)

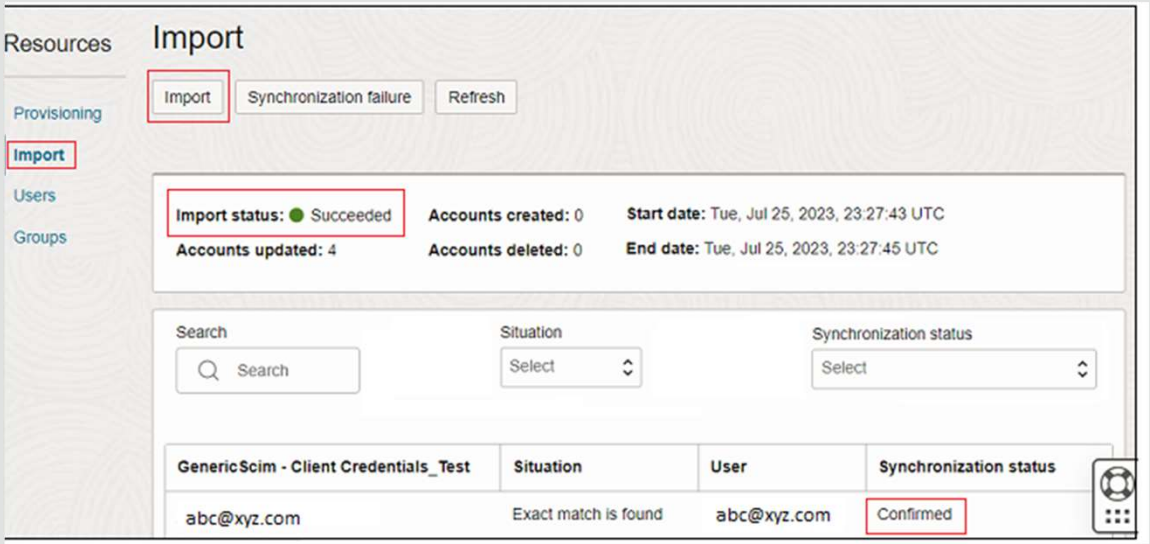
Steps: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/synchronize_with_scim.html

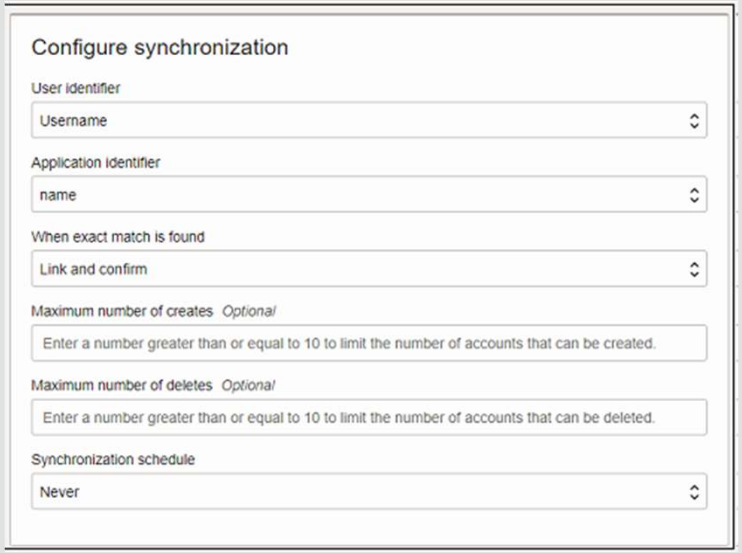




Full Sync and Scheduled Sync

- Full synchronization to make sure that all changes made in the source identity domain are reflected in the target identity domain
- Scheduled sync to make incremental updates in the target domain





Application Group Support

Ability to use EPM application (native) groups to assign application roles

- All users in an application group inherit the roles assigned to the group.

Steps: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/pappm/provuser.html

IDCS Email Notification Customization

- You can modify the notification templates for the email notifications from IDCS for activities, including user addition, role assignment, and password expiry.
- You can select the notification language, the activities for which notifications are to be sent, the email sender, subject, and body.

Steps: https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/customize-oracle-identity-cloud-service-notifications1.html

Avoiding Welcome Email Notifications

Newly Created Users:

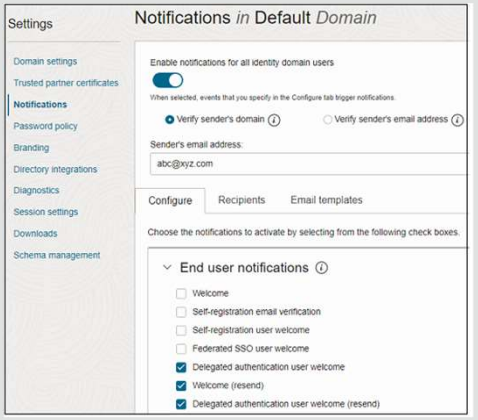
- Import user information from a file in the following format:

User ID,Last Name,First Name,Work Email,Primary Email Type,Federated,ByPass Notification
john.doe@example.com,Doe,John,john.doe@example.com,WORK,TRUE,TRUE
jdoe,Doe,Jane,jane.doe@example.com,WORK,TRUE,TRUE

Make sure that Federated and ByPass Notification fields are both set to TRUE.

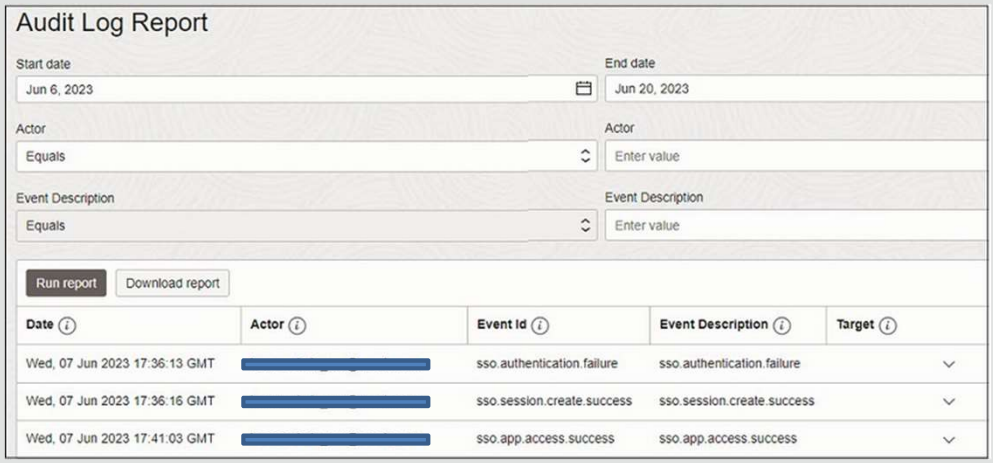
Users Created through Cloning:

- Turn off activation emails



Accessing Audit and User Reports

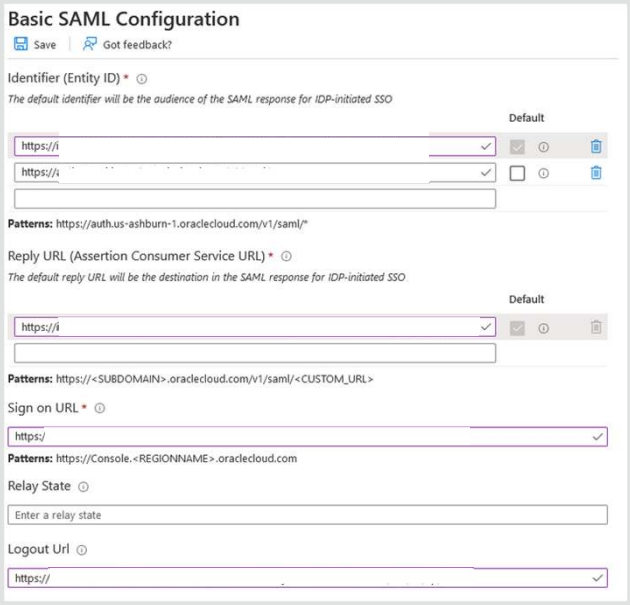
- Reports for successful and failed logins, notifications delivery status, user sign-in and sign-out activity, application access information and diagnostics data
- Retention period of 30 (default), 60 or 90 days
- Available via **console** (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/accessing_audit_and_user_reports_in_identity_cloud_service.html) or **REST API** (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/idcs_audit_login_reports_rest_apis.html)

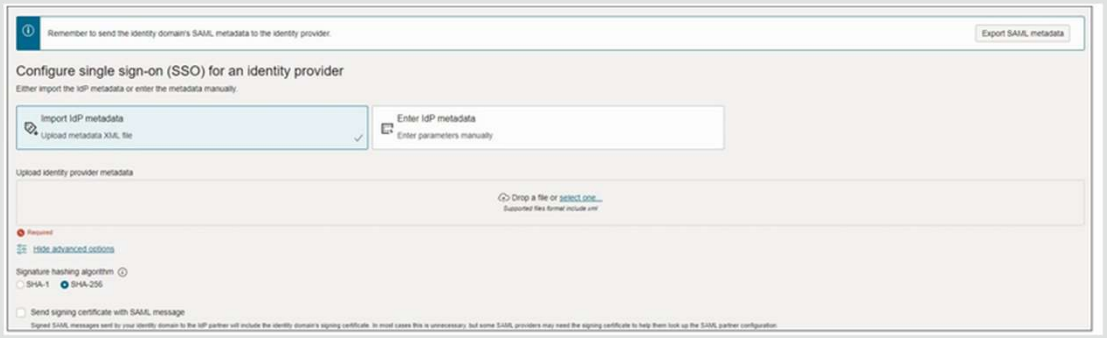


SSO (Single Sign-On)

- Support of all SAML 2.0-compliant Identity Providers (IdP)

Steps: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/3_sso_config_section_header.html

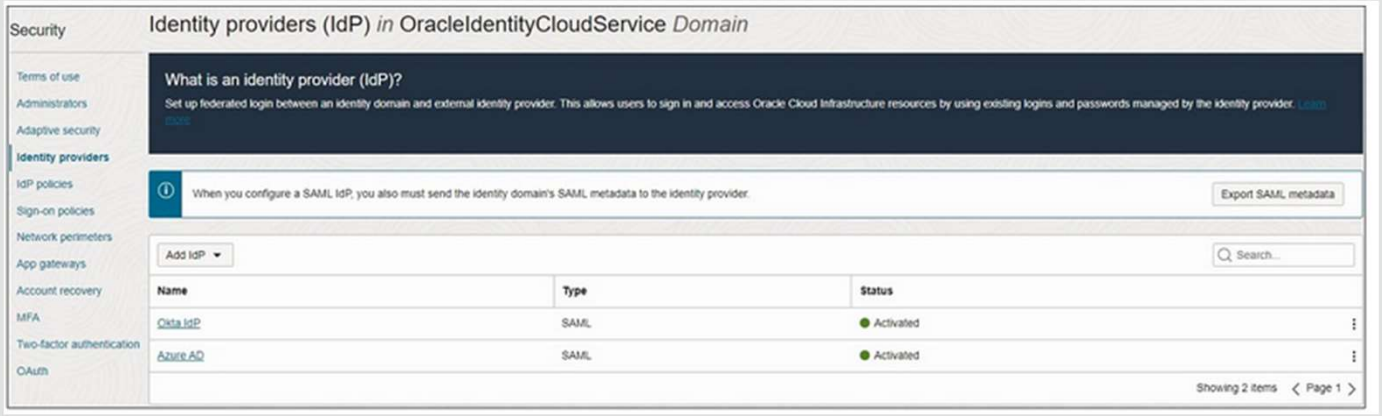




Support of Multiple Identity Providers in a Domain

- Support of multiple IdPs for a domain
- Ability to choose the IdP to SSO with

Steps: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/comfigure_multiple_idp_iam.html



IP AllowList Support

Ability to allow requests from only selected IP addresses to be processed by the EPM Cloud environment

- **EPM Automate**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_ip_allowlist.html
- **REST API**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_update_ip_allowlist_oci.html

Ensure to add the outbound IP addresses of the regions of other services, if you want EPM Cloud to accept requests from them.

- List of IP addresses for different regions: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/outbound_ip_address_cloud_dc.html

OAuth2 Support

- In addition to Basic Auth, OAuth2 is supported for EPM Automate, REST API, and EPM Integration Agent

OAuth2 Setup: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/authentication_oath.html

Virus Scan on Uploaded Files

- Disabled by default

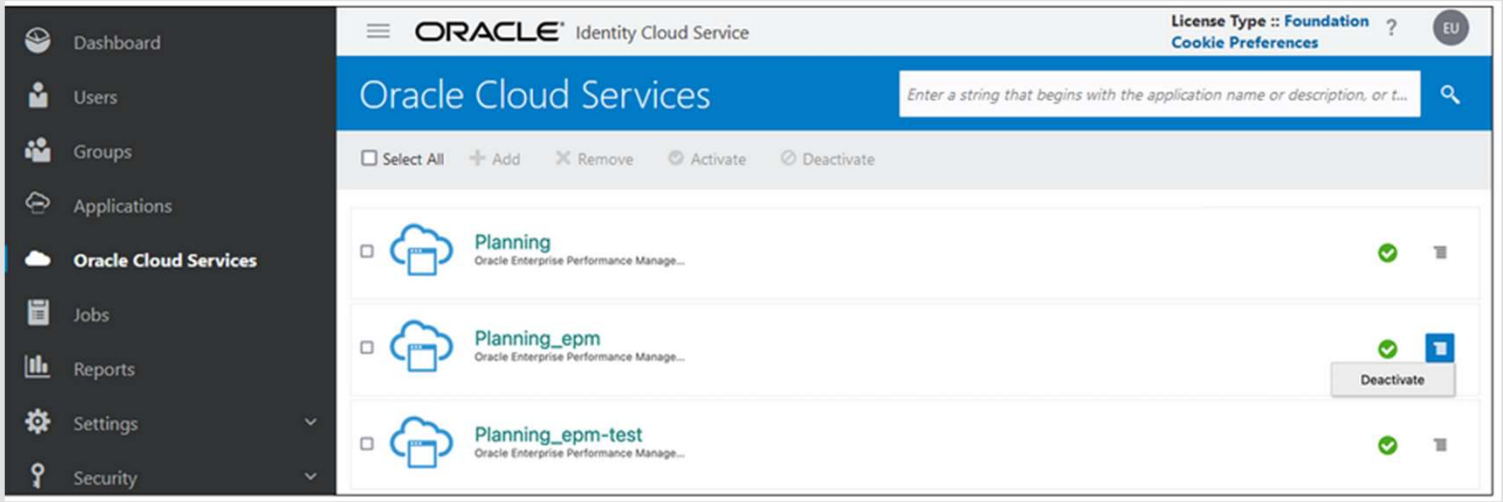
- Enable it via EPM Automate or REST API
  - **EPM Automate**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_virus_scan_onfile_uploads.html

  - **REST API**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_set_virus_scan_on_file_upload.html

Deactivating Access to an Environment

An environment can be deactivated so that no user can log in to them.

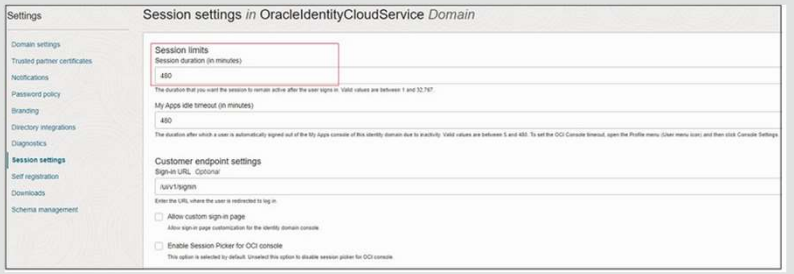
- Use this feature when an environment is not in use or when you don't want anyone to sign into an environment.
- It can also be used when you need to quickly deactivate access to an environment due to an internal or external security threat that needs to be investigated.



Idle Session Timeout and Maximum Session Duration

- Set idle session timeout via EPM Automate (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_idle_session_timeout.html) or REST API (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/set_idle_session_timeout.html)

- Set maximum session duration via Cloud Console.



The maximum session duration is not the same as the idle session timeout. Even if the session is active, EPM Cloud will log the users out after the maximum session duration is reached.

Blocking Connections from Specific Countries, or Allow Connections from Specific Countries Only

Create a Service Request to:

- Block connections from specific countries (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/sop_request_country_connects.html), or
- Allow connections from specific countries only (https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/sop_request_allow_secific_country_connects.html)

SPF (Sender Protection Framework) and DKIM (DomainKeys Identified Mail) Support

- EPM Cloud environments publish the SPF policy that identifies the Oracle server IP addresses and subnets that are permitted to send cloud services emails.
  - You can use the SPF policy information to assess the validity of the messages to determine whether or not to accept them. Additionally, you can use the information as a part of the message protection services.

  Configuring SPF record: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/6_house_keeping_tasks_spf_email_verification.html

- EPM Cloud email servers sign outgoing messages using a private key. Receiving mail servers then use a public key published on the oraclecloud.com DNS record to verify the signatures on the email message.

  Steps for DKIM: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cgsad/6_house_keeping_tasks_dkim_support_epm_cloud_oci.html

BYOK (Bring Your Own Key) Support

- Specify a custom encryption key used to encrypt database access credentials in EPM Cloud
- Set it via:
  - **EPM Automate**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_encryption_key.html
  - **REST API**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_set_encryption_key_v2.html

Control Manual Data Access

- In emergency situations, Oracle resorts to an internal process whereby a high-level development executive, after an independent verification process, permits manual access to the relational and Essbase databases.

- You can stop Oracle from accessing these databases without your explicit approval. Additionally, you have the option to prohibit Oracle from manually accessing the relational and Essbase databases in emergency situations even if a service request is open.

- Do it via:
  - **EPM Automate**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_manual_db_access.html
  - **REST API**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_manage_permission_for_manual_access_to_database_v2.html

Setting the Start Time of Daily Maintenance

You can setup the daily maintenance start time, using:

- Daily Maintenance user interface
- **EPM Automate command**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_daily_maint_start.html

- **REST API:** https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_update_maintenance_time_v2.html

Daily Backup Archival, Retention, and Retrieval

- All EPM Cloud environments create daily backups.
- Daily backups are archived to Oracle Object Storage.
- Production environment backups are retained for 60 days while test environment backups are retained for 30 days.
- You can use self-service operations to check for and copy available backup snapshots from Object Storage to your environment.
  - **EPM Automate commands:**
    - List Backups: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_list_backups.html
    - Restore Backup: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_restore_backup.html
  - **REST APIs:**
    - List Backups: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_list_backups_oci.html
    - Restore Backup: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_restore_backup_oci.html

Activity Report

Enables Service Administrators to understand application usage and helps streamline application design by identifying user requests, calculation scripts, forms, reports, etc.

Two versions of the report:

- HTML version for manual viewing
- JSON version for programmatic parsing

Retained for 60 days

- Archive them if you want to know historical trends.

Generated in these situations:

- Every day during daily maintenance of the service
- Each time you submit a Provide Feedback submission
- Every time you execute the resetService EPM Automate command to restart an environment

Activity Report Content

- Information About Your Environment
- User Information
- Interface Usage and Response Data
- Operational Metrics
- Jobs in the Last Hour
- Application Size Information
- Essbase Statistics
- Calculation Script Statistics
- Manual Database Access Information
- Manual Essbase Access Information
- Business Rules Information
- Application Design and Runtime Information
- Account Reconciliation Metrics
- Enterprise Journal Runtime Metrics
- Profitability and Cost Management Design and Runtime Metrics
- Supplemental Data Manager Design and Runtime Metrics
- Task Manager Design and Runtime Metrics
- Most Recent Metadata Validation Errors and Warnings
- Consolidation and Translation Jobs Statistics
- Reports and Books Execution Statistics
- CPU and Memory Usage Statistics
- Browser,Smart View, and Excel Usage Information

EPM Cloud Operations Guide

EPM Cloud Operations Guide is a one-stop shop for:

- Best practices
- Troubleshooting any issue
- Process to contact Oracle for any issue, request, or question
- Understand EPM Cloud Change Management Process

Location: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/index.html

EPM Cloud Operations Guide

4 Troubleshooting EPM Cloud Issues

This section provides troubleshooting tips for various Oracle Enterprise Performance Management Cloud issues. It also lists the information you should provide to Oracle when seeking help if the troubleshooting tips do not resolve the issue.

In this Section

BSO and ASO Cube Best Practices

How to optimize BSO cubes:
https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/op_procs_bso_defrg_plan_type.html

How to optimize ASO cubes:
https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/tsepm/op_procs_optimize_aso_retrieval.html

Set Essbase Query Governor

By default, an Essbase query can run indefinitely (until terminated by the daily maintenance).

To avoid runaway query, set the maximum amount of time that an Essbase query can use to retrieve and deliver information before it is terminated

- **EPM Automate command**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/cepma/epm_auto_set_essbase_governor_time.html
- **REST API**: https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/prest/lcm_set_essbase_query_governor_execution_time.html

Thank You