Oracle® Fusion Cloud EPM

Getting Started Guide for Administrators

E96235-100

Oracle Fusion Cloud EPM Getting Started Guide for Administrators,

E96235-100

Primary Author: EPM Information Development Team

Contents

3 Working with Subscriptions

4 Migrating to Cloud EPM and Cloud EDM

7 Managing Users and Groups in OCI IAM

8 Configuring Security Settings

A Frequently Asked Questions

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Documentation Feedback

To provide feedback on this documentation, click the feedback button at the bottom of the page in any Oracle Help Center topic. You can also send email to epmdoc_ww@oracle.com.

1

Creating and Running an EPM Center of Excellence

A best practice for EPM is to create a CoE (Center of Excellence).

An **EPM CoE** is a unified effort to ensure adoption and best practices. It drives transformation in business processes related to performance management and the use of technology-enabled solutions.

Cloud adoption can empower your organization to improve business agility and promote innovative solutions. An EPM CoE oversees your cloud initiative, and it can help protect and maintain your investment and promote effective use.

The EPM CoE team:

- Ensures cloud adoption, helping your organization get the most out of your Oracle Fusion Cloud EPM investment
- Serves as a steering committee for best practices
- Leads EPM-related change management initiatives and drives transformation

All customers can benefit from an EPM CoE, including customers who have already implemented EPM.

How Do I Get Started?

Click to get best practices, guidance, and strategies for your own EPM CoE: Introduction to EPM Center of Excellence.

Learn More

- Watch the Cloud Customer Connect webinar: Creating and Running a Center of Excellence (CoE) for Cloud EPM
- Watch the videos: Overview: EPM Center of Excellence and Creating a Center of Excellence.
- See the business benefits and value proposition of an EPM CoE in *Creating and Running an EPM Center of Excellence*.

2

Overview

Scope of this Guide

The information contained in this guide applies to both Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management.

In This Section:

About Cloud EPM

Oracle Fusion Cloud Enterprise Performance Management offers the following business processes:

- Account Reconciliation
- Enterprise Data Management
- Financial Consolidation and Close
- FreeForm
- Narrative Reporting
- Planning
- Planning Modules
- Profitability and Cost Management
- Sales Planning
- Strategic Workforce Planning
- Tax Reporting

Account Reconciliation

Reconciliations ensure that a company's financial accounts are validated by checking to see if the balance in the account is correct. Account Reconciliation makes this process simpler and faster for companies by automating the process and helping users involved in the process collaborate effectively.

Because account balances are valid at a point in time, and business conditions change, it is critical that reconciliations occur. In addition, companies face stiff penalties for failing to reconcile.

Account Reconciliation consists of two modules: Reconciliation Compliance and Transaction Matching.

Your Goal	Watch This
Learn more about Account Reconciliation.	Overview Tour Video

Reconciliation Compliance

Reconciliation Compliance helps you manage account reconciliation processes, including balance sheet reconciliations, consolidation system reconciliations, and other reconciliation processes in effect.

Reconciliations can be performed at whatever level makes sense for the business. For example, you could perform some reconciliation by business unit or company code, while performing other reconciliations at the department level. An administrator can create mapping rules to assign the account balances to the reconciliations, and when balances are imported, ensure they appear in the correct reconciliation based on these rules.

The administrator sets up the reconciliation lists that contain the balances to be reconciled, as well as account descriptions, instructions, due dates, and completed dates. Email notifications are sent, reminding other users that due dates are approaching, or that reconciliations can be acted upon.

Transaction Matching

Transaction Matching is an integrated module of Account Reconciliation and the perfect complement to the existing Reconciliation Compliance feature set.

With Transaction Matching, companies can automate performance of high volume/labor intensive reconciliations, and seamlessly integrate those results into the tracking features within Reconciliation Compliance.

This powerful module helps companies save additional time on performing reconciliations while improving quality and reducing risk.

Enterprise Data Management

Enterprise Data Management is a modern, agile data management application that enables enterprises to manage application-specific business viewpoints, govern changes across them, share and map data sets to accelerate cloud deployment, and build an authoritative system of reference.

Enterprise Data Management business process is available for the following types of EPM Enterprise subscriptions:

- Hosted Employee Metric (Unlimited records)
- Hosted Named User Metric (Maximum 5000 records)

> **Note**
>
> The record count represents unique nodes across all applications, grouped by business domains, which are logical groupings of real-world entities. The Enterprise Data Management business process provides enough records for a capability preview only whereas the Oracle Fusion Cloud Enterprise Data Management subscription has no restrictions on hosted employee and record metrics.

For a detailed feature overview, see Features in Enterprise Data Management and Cloud EDM.

Your Goal	Watch this Video
Get an overview of Enterprise Data Management	Overview Tour Video
Understand the user interface of Enterprise Data Management	Overview: User Interface Tour Video

Financial Consolidation and Close

Financial Consolidation and Close is a subscription-based consolidation and reporting solution built for and deployed on Oracle Cloud. It provides a simple and quick deployment for users who want fast implementation with no hardware and minimal IT support. It provides a user-friendly and intuitive interface along with built-in functionality for consolidation and close process tasks.

Financial Consolidation and Close provides these features:

- Simplified tablet user interface
- Native dashboarding and analysis
- Predefined dimensions for detailed analysis
- Flexible application configuration with pre-built forms and reports
- Currency translations and FX adjustment calculations
- Automated cash flow
- Dynamic out-of-box calculations with limited need for customization
- Simplified Consolidation dimension for easy audit
- Close calendar task management and workflow
- Supplemental schedule data management
- Enterprise Journals

Your Goal	Watch this
Get an overview of Financial Consolidation and Close	Overview Tour Video
Get started with the consolidation and close process	Get Started Video

FreeForm

FreeForm is a subscription-based flexible and customizable reporting and planning solution deployed on Oracle Fusion Cloud EPM. It uses the proven, scalable, and best-in-class Oracle SaaS Cloud architecture.

The FreeForm business process helps companies plan their cloud strategy efficiently by avoiding reporting data fragmentation across cloud services or between cloud and on-premises solutions. It delivers instant value and greater productivity for reporting and planning use cases for all lines of business across the company. For more information, refer to Understanding FreeForm in *Administering FreeForm*

Users interact with FreeForm through a web browser or Microsoft Office interface to collaboratively report, analyze, and plan their business needs.

Proven Platform and Technology

The FreeForm functional architecture, which is based on the proven Cloud EPM Platform, provides a unified reporting and planning solution to solve simple to complex use cases across numerous industries. With FreeForm business process, enterprise-wide reporting, close and planning use cases, along with users and their security, can be managed within a centralized place.

Best-in-Class Functionality

With FreeForm business process you can easily create forms, reports, and on-the-fly what-if models with real-time collaborative dashboards. You can also perform ad hoc analysis and create powerful custom reports using annotations, commentary, and document attachments.

Scalable and Flexible

FreeForm leverages the powerful Oracle Essbase OLAP calculation engine and the comprehensive web and Microsoft Office-based Oracle Smart View for Office to enable fast rendering of complex grids with large volumes of data. Inbuilt time and data intelligence provides out-of-the-box spreading and fast on-demand aggregation capabilities. By creating and sharing on-the-fly models, you can quickly build and collaborate using Excel and web interfaces.

Enterprise Ready

FreeForm is a one-stop business process to seamlessly plug in a flexible and customizable modeling and reporting solution into larger transaction systems from Oracle and beyond. It supports small-scale to large-scale deployments, data backup and migration. It also provides Enterprise Resource Planning (ERP) data integration capabilities without compromising ease of use or self-service for smaller customers. It provides flat file and Excel-based import and export, and comprehensive mapping capabilities for more sophisticated data integration use cases. You can seamlessly load and extract information, and drill back to any source ERP system.

Essbase Portability

Existing FreeForm customers can leverage built-in migration capabilities to port their on-premises Essbase application to the FreeForm business process to have a SaaS-based deployment of these Essbase cubes. This capability enables organizations to pursue a cloud first strategy for reporting and planning.

Unified Deployment

The FreeForm business process lets you report, analyze and plan within a unified construct. Your Oracle Fusion Cloud Enterprise Performance Management subscription includes everything that you need from a reporting and planning standpoint using web and Smart View interfaces. You don't need to license, install, upgrade, or patch software; you don't have to buy, install, or configure hardware. FreeForm enables you to leverage the deep product expertise of the worldwide Oracle Hyperion Partner network to develop and deploy cloud-based applications in just weeks.

Narrative Reporting

Narrative Reporting is an Oracle Cloud solution for management and narrative reporting. It provides a secure, collaborative, and process driven approach for defining, authoring,

reviewing and publishing financial and management report packages. In addition, Narrative Reporting offers multidimensional analytics, and you can choose to store, analyze, and source data from the Cloud via built-in analytics or use your own existing data sources for analyzing and authoring doclet content.

Key benefits:

- **Combine Data and Narrative:** Use report packages and doclets to address authoring, collaboration, commentary, and delivery needs.
- **Collaborate Securely:** Gives report contributors access to content based on their role and insures that sensitive content is secure. Also, lets report owners see the progress of the reporting lifecycle.
- **Report Confidently:** Allows you to trust that the data is reliable and accurate while providing faster, more accurate insights to all stakeholders.

Your Goal	Watch This
Learn more about Narrative Reporting.	 Overview Tour Video

Planning

Planning is a subscription-based planning and budgeting solution built for and deployed on Oracle Fusion Cloud EPM, using a proven, flexible planning and reporting best-in-class architecture. It delivers instant value and greater productivity for business planners, analysts, modelers, and decision-makers across all lines of business of an enterprise. Users interact through a Web 2.0 or Microsoft Office interface to model, plan, and report. The service, built to scale and perform, uses industry-standard Cloud EPM infrastructure.

Proven Platform and Technology

The service helps companies plan their cloud strategy efficiently by avoiding data and business process fragmentation. It is built to optimize Oracle Fusion Cloud Enterprise Performance Management resources. The service's functional architecture is based on the proven Planning platform, which helps solve simple to complex planning use cases across numerous industries. In Cloud EPM, enterprise-wide user profiles can be maintained in one place so that they can be reused across all Cloud EPM Services to which an organization subscribes.

Best-in-Class Functionality

The service offers an intuitive Web 2.0 and Microsoft Office interface for driver-based modeling, rolling forecasts, and management reporting for time-sensitive and goal-oriented planning activities. You can easily create and share on-the-fly models and validate them against sophisticated statistical predictive capabilities, thus generating unbiased, accurate, and agile plans. This service is built for real-time collaborative planning and variance analysis across the enterprise, using powerful annotations, commentary, document attachments, tasks, workflow, and reporting capabilities.

Scalable and Flexible

The service leverages the powerful Essbase OLAP calculation engine and a comprehensive rules framework to enable fast processing of complex calculations for large volumes of data. Time and data intelligence built into the service provides out-of-the-box spreading and fast on-demand aggregation capabilities. By creating and sharing on-the-fly models, you can quickly build and collaborate using Microsoft Excel and Web interfaces.

Enterprise Ready

The service is a one-stop cloud service to build, deploy, and manage business planning activities for any size organization. It supports small- to large-scale deployment, data backup and migration, plus packaged Enterprise Resource Planning (ERP) data integration capabilities without compromising ease of use or self-service for smaller customers. This service includes comprehensive features to raise issues, get support, and seek product enhancements. It provides flat-file and Excel-based import and export, and comprehensive mapping capabilities for more sophisticated data integration use cases. You can seamlessly load and extract information, and you can drill back to source ERP.

Rapid Deployment

The service lets you get started immediately, because it requires no initial investment. Your subscription includes everything that you need. You don't need to license, install, upgrade, or patch software. You don't have to buy, install, or configure hardware. You can also leverage the deep product expertise of the worldwide Oracle Hyperion Partner network to develop and deploy cloud-based planning applications in weeks, using quick-start templates.

Portability

Existing Planning customers can leverage built-in migration capabilities to port their on-premises Planning application to the service. This capability also enables organizations to introduce or extend Planning usage across the enterprise to other lines of businesses without additional demands on their Information technology resource and budgets.

Your Goal	Watch This
Learn more about Planning.	Overview Tour Video

Planning Modules

Planning Modules comprise complete planning and budgeting solutions for Financials, Workforce, Capital, and Projects. These business processes include built-in best practice predefined content including forms, calculations, dashboards, drivers, and key performance indicators (KPIs). Forms are designed to integrate with the dashboards and reports that dynamically reflect your data, plans, and forecasts.

Your Goal	Watch This
Learn more about Planning Modules.	Overview Tour Video

Financials

The Financials solution provides integrated driver-based planning for income statement, balance sheet, and cash flow. The out-of-box tools, such as KPIs, drivers, and accounts help you prepare reports faster. You can also use Financials to perform expense and revenue planning.

Your Goal	Watch This
Learn more about Financials.	Overview Tour Video

Workforce

The Workforce solution enables headcount and compensation planning to link financial plans with the workforce plan. You can budget for future headcount and related personnel expenses such as salary, benefits, and taxes.

Your Goal	Watch This
Learn more about Workforce.	 Overview Tour Video

Projects

The Projects solution bridges the gap between project planning systems and the financial planning process. It helps you assess the impact organizational projects and initiatives have on overall resources to ensure they align with short and long term financial targets.

Your Goal	Watch This
Learn more about Projects.	 Overview Tour Video

Capital

The Capital solution helps you plan for the long-term impact of capital assets on financial plans to manage, prioritize, and plan for capital expenses.

Your Goal	Watch This
Learn more about Capital.	 Overview Tour Video

Strategic Modeling

The Strategic Modeling solution combines a set of rich financial forecasting and modeling features with built in on-the-fly scenario analysis and modeling capabilities for long-term strategic planning.

Your Goal	Watch This
Learn more about Strategic Modeling.	 Overview Tour Video

You might not see all the features described in this guide depending on what your Service Administrator has enabled. Service Administrators can incrementally enable some features, which adds additional forms, dashboards, KPIs, rules, and so on.

Profitability and Cost Management

Businesses must be able to accurately measure, allocate, and manage costs and revenue to maximize profitability. Profitability and Cost Management manages the cost and revenue allocations necessary to compute profitability for business segments, such as products, customers, regions, and branches. It enables you to use cost decomposition, consumption-based costing, and scenario-playing to measure profitability for effective planning and decision support.

The Profitability and Cost Management business process is now available as the following two separate applications:

- About Profitability and Cost Management
- Enterprise Profitability and Cost Management

Enterprise Profitability and Cost Management, a more modern implementation of the features available in Profitability and Cost Management, provides seamless integration with other Oracle Fusion Cloud Enterprise Performance Management components.

About Enterprise Profitability and Cost Management

Enterprise Profitability and Cost Management, an updated version of Profitability and Cost Management. It provides these features to analysts who have deep domain experience in the computation and reporting methods of management reporting, but may not have much experience with scripting or programming languages.

Building Allocation Models

Enterprise Profitability and Cost Management provides a point and click modeling interface to build complex waterfall processes of allocation custom calculation rules. Complex waterfalls consisting of hundreds of rules organized in a sequentially controlled model can be applied to data across many periods or forecast ranges.

Managing the Calculation Process

Enterprise Profitability and Cost Management provides simple process execution controls to run all or a part of a model and reverse the results of previous runs if necessary. It provides a complete calculation history and supports review of model logic, calculation results, and performance statistics for any given point in time.

Integration with Financial and Planning Systems

The flexible design structures of Enterprise Profitability and Cost Management allow the models to combine dimensions and data from multiple source systems to support reporting that requires merging of data from many financial and operational systems. Enterprise Profitability and Cost Management's design flexibility and integration capabilities allow it to aggregate allocation processes for many financial and reporting systems into a common functional allocation hub.

Transparency of Results

Calculation audit reports for logic changes, performance statistics, and a rule-by-rule tracking of results provide complete transparency. Detailed rule transaction results available in Enterprise Profitability and Cost Management allow tracing the source of any allocated value.

Your Goal	Watch This
Get an overview of Enterprise Profitability and Cost Management.	Overview Tour Video
Get started with Enterprise Profitability and Cost Management	Feature Overview Tour
Learn about Enterprise Profitability and Cost Management models and modeling	Overview Video

About Profitability and Cost Management

Profitability and Cost Management application models are designed for use by analysts who have deep domain experience in the computation and reporting methods of management reporting, but may not have much experience with scripting or programming languages.

Your Goal	Watch This
Learn more about Profitability and Cost Management.	 Overview Tour Video

Profitability and Cost Management applications data is housed in both multidimensional databases and relational databases.

Sales Planning

Sales Planning enables you to automate critical processes by eliminating spreadsheets in key sales operations processes and improves collaboration for planning and modeling sales quotas. Sales Planning is available with EPM Enterprise as an application type in the Planning business process.

Sales Planning is extensible using the Cloud EPM Platform framework to further add additional configurations and personalization into your sales planning application with custom navigation flows, dashboards, and infolets.

Use tasks and approvals to manage the quota planning process. Use Groovy rules to customize even further for enhanced calculation and business rules. Sales Planning can be integrated with Oracle Engagement Cloud – Sales Cloud for pushing quota targets to incentive compensation or bring in actual attainment.

Your Goal	Watch This
Learn more about Sales Planning.	 Overview Tour Video

About Quota Planning

The Quota Planning business process offers top-down and bottom up target quota planning by territory, product, account, or other custom dimensions. Use Predictive Planning and what-if scenario planning to explore and compare different quota scenarios for informed decision making. Quota Planning builds best practices into its content, including its forms, calculations, dashboards, infolets, drivers, and measures.

Quota Planning helps you plan reliable target quotas by engaging all of the participants of the process, for example, the VP of Sales, Sales Operations, Sales Managers, and Sales Reps. Set a target quota for the next year. Then, optimize your results by making adjustments by product, applying padding or seasonality, or performing predictive planning or what-if analysis. When the target is ready, planners perform top-down or waterfall planning to allocate the target quota throughout the hierarchy.

If needed in your organization, you can also perform bottom up planning to get quota commitments from Sales Reps, allowing a collaborative approach. After the target quotas are pushed up to the next level of the hierarchy and aggregated, you can compare top down and bottom up results. Use the built-in dashboards to analyze and evaluate your quota plans with quota attainments.

Enhance the planning process in your organization by adding additional measures, task lists, or approvals.

Your Goal	Watch This
Learn more about Quota Planning.	 Overview: Quota Planning in Sales Planning

About Advanced Sales Forecasting

Advanced Sales Forecasting provides a robust platform for the sales forecasting process, allowing multidimensional sales forecasting across territory, products, accounts, channels, or other custom dimensions. It offers sales teams connected sales planning with integration between Quota Planning, compensation planning, and sales forecasts. With Advanced Sales Forecasting, you can plan at the weekly or monthly level, and use a rolling forecast if your business requires it. It offers these key features:

- Out-of-box best practice content for sales forecasting and analysis, including metrics, KPIs, and measures to help data-driven sales forecasting across the Sales hierarchy.
- Extensibility using the Planning Cloud platform, allowing additional configurations, such as custom forms and dashboards, measures, dimensions, navigation flows, and Groovy rules for custom calculations.
- Ability to adjust forecast commitment at the territory level or detailed level (for example, by product or account) to facilitate collaborative data-driven forecast commitment.
- Predictive Planning to take the guesswork out of your forecasting.
- Oracle Smart View for Office, which provides a common Microsoft Office interface designed specifically for Oracle Fusion Cloud Enterprise Performance Management, including Sales Planning.
- Instantaneous aggregations and reporting using out-of-box reporting cube.

Advanced Sales Forecasting ensures greater reliability in your forecasts, and accountability and collaboration between Sales Management and Sales Reps.

About Key Account Planning

Key Account Planning expands Sales Planning to cover a data driven approach to sales baseline planning and impact of trade promotions on sales plans. This results in an overall view of the customer profit and loss including an assessment of promoted and non promoted volume and revenue by customer and product group. Key Account Planning helps key account managers plan trade promotion strategies in order to optimize their trade spends and offers collaborative sales planning. By using baseline planning and promotion planning, key account managers or sales managers can perform gap analysis and see the uplifts - the impact on sales volume or revenue - from running trade promotions.

You'll perform these tasks in Key Account Planning:

- Perform baseline planning. Run predictions on your forecast by key account and product segment, perform what-if scenario modeling, and make adjustments.
- Then, in your baseline plan, use building blocks such as different pricing, placements, and product variants to identify the additional non promotional sales plan adjustments.
- Next, add, analyze and adjust trade promotional activities to strategically close the gap between your target and plan, identifying each promotion’s incremental uplift volume on an account, trade spends and profit and loss, including additional contract measures specified for the customer and COGS, to get a full view of customer profit and loss.

- Last, review volume and revenue plans and analyze trade spends and historical promotions to inform your key account planning and other sales planning decisions.

Key functionality includes:

- Baseline Planning including built-in Predictive Planning
- Integration with Quota Planning to bring in targets
- Gap Analysis – Target versus Baseline
- Trade Promotion Planning
  - Promotions planning by dates that drive the volumes and trade spends to corresponding months based on specified uplifts
  - Promotional What-ifs
  - Variable spending. These calculations cover taking the variable cost and applies them to promoted period volumes
  - Promotional planning use cases
    - Promotion spanning across periods
    - Promotions for single or multiple products
    - Multiple promotions for the same product in a period
    - Multiple promotions for the same product with overlapping dates
  - Adjustments to uplifts by Products
- Trade Spend Summary and ROI on Uplift and Revenue
- Customer Profit and Loss
  - By Customer and Product Group
  - Revenue and Uplift Revenue
  - Trade Spends – Variable and Fixed
  - COGS
  - Contract measures
- Analytics
  - Overview Dashboards with KPIs and visualization
  - Promoted and Non promoted volumes across the customer / product/ territory hierarchy
  - Key Account Summary

Key Account Planning connects sales planning with trade promotions marketing campaigns to increase sales volume or revenue. Key Account Planning:

- Provides forecast accuracy and reliability with data-driven sales plans for customer and product groups including trade promotions.
- Fosters collaboration and accountability.
- Helps you evaluate right promotion strategies by analyzing the effectiveness of your trade promotions.
- Offers what-if scenario planning to evaluate different promotion strategies.
- Eases the pain of managing multiple spreadsheets.

- Offers an extensible framework based on a robust Planning Platform and ability to integrate with Sales Cloud.

Your Goal	Watch This
Learn more about Key Account Planning.	 Overview: Key Account Planning in Sales Planning

Strategic Workforce Planning

Strategic Workforce Planning translates long-term corporate strategy into execution plans by ensuring that the strategy is supported by the right workforce—the right skill sets and headcount at the right time. Strategic Workforce Planning is available with EPM Enterprise as an application type in the Planning business process.

Strategic Workforce Planning is extensible using the Cloud EPM Platform framework to further add additional configurations and personalization into your Strategic Workforce Planning application with custom navigation flows, dashboards, and infolets.

You look at long-term demand for resources by exploring scenarios that impact those demands. You also look at what's going to happen with your current workforce, for example, through retirement or natural attrition. Evaluating demand against supply helps you understand what gaps there may be—positive or negative—so that you can proactively plan for needed resources. You can anticipate the headcount and skills needed to support your business strategy.

Strategic Workforce Planning provides configurable drivers and demand thresholds that enable planners to answer such questions as, "Do our employees have the right skill sets to accomplish future plans?" and "Will expected expenses and revenues support our plans?". You select the best calculation logic for each driver, which translates driver values to future long-term full-time equivalent (FTE).

Watch this video to learn about Strategic Workforce Planning.

 Overview Tour Video

You can also enable Workforce to manage and track headcount expenses. You can then align critical corporate resources—people and dollars—with the strategies that best leverage a competitive advantage. Departments can collaborate to plan headcount and related expenses such as salaries, health care, bonuses, and taxes. Planners can see up-to-date graphics that show expenses and trends.

If Workforce is enabled with all its features, planners can manage and track headcount expenses:

- Analyze, calculate, and report on headcount, salary, bonuses, taxes, and health care expenses
- Plan for hires, transfers, promotions, terminations, and so on
- Define country-appropriate taxes and benefits

Tax Reporting

Tax Reporting is a comprehensive global tax provision solution for multinational companies reporting under GAAP (Generally Accepted Accounting Principles) or IFRS (International Finance Reporting Standards). The solution encompasses all stages of the corporate tax

provision process, including tax automation, data collection, tax provision calculation, return-to-accrual automation, tax reporting and analysis, and Country by Country (CbCR) reporting.

Tax Reporting calculates your company's global tax provision, effective tax rate, and deferred tax for tax provisioning purposes. The application complies with the standards for accounting for income taxes under US GAAP and IFRS.

Tax Reporting can use the same platform as your corporate close process and therefore may be directly integrated utilizing the same metadata. As one solution, consolidated pretax income can be reported by legal entity to calculate the consolidated income tax provision. When corporate accounting finalizes the period-end close and all required amounts—such as permanent and temporary differences, tax rates, and foreign exchange rates—Tax Reporting automatically calculates the current and deferred income tax provisions by legal entity and by jurisdiction.

From the provision calculation, Tax Reporting produces a journal entry and draft income tax financial statement disclosure, complete with supporting schedules. The supporting schedules provide details for the required disclosures in the income tax footnote to the financial statements, including:

- Pretax income by foreign and domestic entities
- Consolidated tax provision by current and deferred tax expense
- Consolidated and statutory effective tax rate reconciliations
- Composition of deferred tax assets, liabilities, and valuation allowance (as required)

Your Goal	Watch This
Learn more about Tax Reporting.	Overview Tour Video

About Cloud EDM

Oracle Fusion Cloud Enterprise Data Management, a stand-alone Oracle Cloud offering, helps manage and govern changes to master, reference, and metadata across the enterprise. Users access enterprise data through portals called viewpoints, govern changes across them via requests, synchronize alternate business perspectives via subscriptions, and map data sets through parent-child relationships and complex multi-dimensional combinations.

You use Cloud EDM to build an authoritative system of reference that orchestrates structural changes to accelerate business transformations, de-risk mergers and acquisitions, stimulate trustworthy business analytics, promote compliance to standards, and build alignment between how a business runs its operations, measures performance, and plans for the future.

Cloud EDM has no restrictions on hosted employee and named user metrics. In contrast, the Enterprise Data Management business process available with the EPM Enterprise subscription is limited to a maximum of 5000 records.

For a detailed feature overview, see Features in Enterprise Data Management and Cloud EDM.

Your Goal	Watch this Video
Get an overview of Cloud EDM	Overview Tour Video
Understand the user interface of Cloud EDM	Overview: User Interface Tour Video

Features in Enterprise Data Management and Cloud EDM

Work with Applications

Application creators register each connected business application to generate end user experiences called a default view. Upon registration, creators can assign others as application owners or data managers. Each view contains one or more viewpoints that are optimized to maintain each registered application dimension as a list or a hierarchy. To collaborate, application owners and view owners may then come together to tailor custom views and viewpoints (for example, by subject area or by business domain) to build change management views. Data managers may then apply changes within their purview.

Work with Views and Viewpoints

Views are end user portals into enterprise data. Browse or search viewpoints within or across views. Import dirty dimension data into viewpoints from contributing applications, validate and resolve issues to build an authoritative system of reference. Compare viewpoints side-by-side to understand differences. Align related properties visually and copy values. Create requests to share data across viewpoints. Use subscriptions to share data between viewpoints by subscribing a target viewpoint to a source viewpoint. When an update is made to the source viewpoint, a request is automatically generated to make the same change in the target viewpoint.

Manage Change with Requests

Requests represent the fundamental building block of change. Use requests to model changes to any viewpoint. Visualize all changes against the target viewpoint, validate them, analyze impact, and only then commit them. Author changes interactively or in batch from file sources. Browse request activity to audit committed changes.

Collaborative Workflows

Collaborative workflows support a submit process, approval process and address these governance challenges:

- Configure one or more approval policies at the application, dimension, hierarchy set, or node type level. The workflow orchestrates the invitation of approvers while executing approval policies concurrently to achieve high quality outcomes.
- Implement request workflows across multiple business contexts to secure approval for related changes across applications.
- Use approvals with subscription requests to simulate application dimension-level enrichment and approval stages across multiple application contexts.
- Define items within a request that are validated, approved, and committed together. This creates integrity in change management and enables change control.

Create Alternate Views and Viewpoints

Tailor custom views and viewpoints to build alternate hierarchies, access read-only reference data for comparison purposes, or work with hierarchy members in a list. Copy viewpoints to make a historical snapshot, perform a what-if scenario, or reorganize data as fit-for-purpose.

Information Model

Each viewpoint is powered by a data chain that specifies associated business objects (using node types), associated parent child relationships (using relationship sets), and associated

predicates such as top nodes (using node sets) to construct each viewpoint for end use. Viewpoints are grouped together logically in views that either represent business applications or subject areas. Application views are defaulted based upon application registration.

Build Data Maps

Create new data chains to manage mapping relationships. Construct mapping viewpoint to map one or more sources to each target application dimension. Compare source to target and create requests to build data maps across applications. Configure mapping keys and locations for each target dimension to export data maps.

Application Integration

Accelerate integration with Oracle Fusion Cloud Enterprise Performance Management applications, for example, Planning, Financial Consolidation and Close, E-Business Suite General Ledger and Oracle Financials Cloud General Ledger, using predefined application registration. Leverage a custom application registration using an open interface to integrate with all other business applications. Use a wizard-driven configuration experience to onboard applications: establish reusable connections, configure import and export operations, and construct ready-to-use, application-specific views for immediate application maintenance purposes.

Automate Tasks

Automate tasks interactively or via a scheduled process using EPM Automate. For example, migrate across service environments, upload and download files, reset an environment and re-create an environment.

Audit Transaction History

Transaction history can be audited to see changes made to nodes, properties, and relationships over time. Transaction history is recorded when requests are committed. You can view, filter, and download transaction history to a file.

Expressions for Custom Business Logic

Expressions are used to define custom business rules for nodes in particular applications. Expressions can be configured for derived properties and property transformations to calculate property values for nodes in viewpoints. Expressions are defined in a graphical manner using a palette and an editor.

Infrastructure Overview

In This Section:

Key Concepts

Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) delivers highly available computing power and infrastructure to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management. When you purchase new subscriptions, you are provided a tenancy in OCI to provision and maintain your environments. During the order activation

process, you can create a tenancy, or if you already have a tenancy, you can assign your subscription to an existing one. After the subscription is assigned, you are ready to create the environments.

Oracle Cloud Console

Oracle Cloud Console is an innovative, fully integrated OCI service that offers self-service capabilities for managing the full lifecycle of your Cloud EPM and Cloud EDM environments. It includes features previously available through My Services, and more. Key functionalities include:

- Creating production and test environments
- Viewing environment information
- User and security management (through IAM)
- Accessing Usage Reports
- Accessing Compliance Reports

Cloud Account Name

The name of the account that manages your subscription. This account is set up when you activate your subscription. Any subscriptions can be activated into one cloud account. The **Cloud Account Name** is your tenancy. This value, which cannot be changed, is visible in your login URLs.

Identity and Access Management (IAM)

IAM is the service that provides authentication and authorization for OCI resources. See Overview of IAM. You interact with the IAM service when you create users, groups, and policies to manage your environments without worrying about setting up any infrastructure or platform details. This is done using the Oracle Cloud Console.

Identity Domain

A slice of the shared identity management infrastructure where Identity Domain Administrators create and manage users and security. Many subscriptions can be activated to use the same identity domain.

Each OCI IAM identity domain serves as an independent identity and access management solution, designed to manage Cloud EPM and Cloud EDM environments. You have the flexibility to create multiple domains and organize your environments across different identity domains.

Features Available only in OCI (Gen2) Cloud EPM and Cloud EDM Environments

The following table lists some of the features that are available only in OCI (Gen2) Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

Table 2-1 New Features in OCI (Gen2) environments

Feature	Description
IAM interface	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 Console 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 Console 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 the environment 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 group and then assign predefined roles to the group. Since groups can be synced with Identity Provider groups (such as Microsoft Entra ID) groups), you can even add individual users to Identity Provider groups and assign the predefined roles to these groups in IAM Interface. See Using IDCS Groups to Assign Predefined Roles to Users
Synchronize 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. See Synchronizing Users and Groups Across Identity Domains (Same or Different Cloud Accounts).
Synchronize users and groups from other Identity Management products	You can use System for Cross-domain Identity Management (SCIM) to enable automatic provisioning of users and groups from other Identity Management products (such as, Microsoft Entra ID). See Synchronizing Users and Groups from Microsoft Entra ID to IAM.
Ability to rename the environment	You can change the environment name and, consequently, the URLs of your environments using Oracle Cloud Console. See Renaming or Relocating an Environment.
Ability to relocate the environment	You can relocate the environment to a different region using Oracle Cloud Console. See Renaming or Relocating an Environment.
Private access to Cloud EPM and Cloud EDM	If you have an OCI IaaS subscription in the same region as your 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 *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*.
Multiple Password Policies	You can create multiple password policies and assign them to different Identity Cloud Service groups. For details, see Manage Oracle Identity Cloud Service Password Policies in *Administering Oracle Identity Cloud Service*.

Table 2-1 (Cont.) New Features in OCI (Gen2) environments

Feature	Description
Network Perimeter (IP Allowlist) for the whole domain	You can configure Network Perimeter to set up the IP allowlist for the whole domain. See Setting up Network Perimeter.
Restrict user access	You can deactivate environments so that user cannot sign in to them. See Deactivate Access to Environments. You can also configure a custom sign-on policy to restrict access to users with specific predefined roles. See Sign-On Policies to Restrict Access to Environments. In addition, you can also deactivate specific user accounts. See Deactivate User Accounts in *Administering Oracle Identity Cloud Service*.
Maximum session duration	You can set the maximum session duration in IAM Interface to log out the user, even if the user is actively using the environment. See Maximum Session Duration.
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.
Disallow Service Administrator to assign predefined roles	You can request Oracle to disallow Service Administrator to assign predefined roles. After Oracle implements this request, only Identity Domain Administrator will be able to assign predefined roles. See Prevent Service Administrators from Granting Predefined Roles in *Operations Guide*.
Database encryption using AES-256I	OCI (Gen2) 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 (Gen2) 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 (Gen2) environments are archived to Oracle Object Storage daily. Production and test environment backups are retained for 60 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 (Gen2) 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
Web Application Firewall (WAF) support	In OCI (Gen2) environments, Web Application Firewall (WAF) is available out-of-the-box and protects the environment from many application layer attacks.
DKIM (DomainKeys Identified Mail) support	Supports DKIM for outgoing messages for default or custom sender email address in OCI (Gen2) environments. See DKIM Support.
Customization of Sign-in Page	You can customize the 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.

Table 2-1 (Cont.) New Features in OCI (Gen2) environments

Feature	Description
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.

Information Sources

The following documents contain information on performing functional administrative:

Table 2-2 Information Sources for Service Administrators

Document Title	Description
Operations Guide	Lists some common Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management issues and the procedures to troubleshoot them. Also details the information that you must provide to Oracle Support while seeking help
Administering Planning	Explains how to create and administer Planning applications
Administering Planning Modules	Explains how to create and administer Planning Modules applications
Administering FreeForm	Explains how to create and administer FreeForm applications
Administering Sales Planning	Describes how to create an application and enable and configure Sales Planning
Administering and Working with Strategic Workforce Planning	Details how to configure and administer Strategic Workforce Planning and complete tasks.
Administering Financial Consolidation and Close	Explains how to create and administer Financial Consolidation and Close applications
Administering Tax Reporting	Explains how to create, configure, and administer Tax Reporting applications
Administering Profitability and Cost Management	Explains how to create and administer Profitability and Cost Management applications
Administering and Working with Enterprise Profitability and Cost Management	Explains how to create and administer Enterprise Profitability and Cost Management applications
Setting Up and Configuring Account Reconciliation	Explains how to set up and configure the account reconciliation process in Cloud EPM
Administering Account Reconciliation	Contains information on administering account reconciliation compliance and transaction matching in Cloud EPM
Administering Narrative Reporting	Explains how to administer Narrative Reporting
Designing with Reports	Explains how to administer Management Reporting to create financial and managerial reports
Working with Applications, Models, and Dimensions for Narrative Reporting	Explains how to set up and administer Narrative Reporting applications

Table 2-2 (Cont.) Information Sources for Service Administrators

Document Title	Description
Working with EPM Automate	Contains information about theEPM Automate, which helps you automate many administrative tasks
Administering Access Control	Contains information about using Access Control to manage user groups and generate various reports to understand service usage
Administering and Working with Oracle Fusion Cloud Enterprise Data Management	Explains how to use Cloud EDM to manage all your enterprise data and work with business perspectives.
Administering Migration	Contains information about using Migration to perform administrative tasks on artifacts and to generate reports that identify artifact changes that have taken place over a period
Working with Financial Reporting	Contains information on administering Financial Reporting to support Cloud EPM components
Administering Oracle Fusion Cloud Enterprise Data Management	Describes how to use Data Management to develop standardized financial data management processes and validate data from most source systems.
Administering Data Integration	Describes how to use the Data Integration to integrate data from source systems into Planning and Planning Modules.
Deploying and Administering Oracle Smart View for Office (Mac and Browser)	Describes how to deploy and administer Oracle Smart View for Office (Mac and Browser).
Getting Started with Oracle Smart View for Google Workspace	Describes how to install and get started with Smart View for Google Workspace.

Oracle Cloud Help Center

From the Help Center, you can get user assistance through various resources, including documentation, videos, and tutorials. The Help Center is typically updated on the first Friday of each month. Key areas to explore include:

- Enterprise Performance Management
- Enterprise Data Management

The Help Center features the following options in the navigation pane:

- **How Do I:** Find step-by-step instructions for typical tasks.
- **FAQs:** Find answers to your environment-specific questions.
- **Books**: Access the latest English documentation.
- **Translated Books**: Explore available translated online help and documentation.
- **Videos**: View videos that offer overview and instructions on using application features.
- **Tutorials**: Discover instructional content to help you learn various topics.

Your Goal	Watch this Video
Learn about available user assistance assets	 Overview Tour Video

Your Goal	Watch this Video
Get answers, learn more, and stay current using the Help Center	 Overview Tour Video

Oracle Learning Library

The Oracle Learning Library is dedicated to hosting free instructional content developed by Oracle subject-matter experts.

Use the Search function in Oracle Learning Library to find tutorials, overview videos and Oracle by Example (OBE) tutorials.

Understanding Translation

The user interface, Online Help, and guides are available in many languages.

User Interface

Generally, the user interface is translated into Arabic, Danish, German, Spanish, Finnish, French, French Canadian, Italian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese (Brazilian), Russian, Swedish, Turkish, Simplified Chinese, and Traditional Chinese.

Exceptions:

- Profitability and Cost Management user interfaces are not translated into Arabic and Norwegian.
- Account Reconciliation and Oracle Fusion Cloud Enterprise Data Management user interface is translated into these additional languages: Czech, Hebrew, Hungarian, Romanian, and Thai.
- Oracle Smart View for Office user interface is translated into these additional languages: Czech, Greek, Hebrew, Hungarian, Portuguese, Romanian, Slovak, and Thai.
- Oracle Digital Assistant for Enterprise Performance Management user interface is available in English only.

> **Note**
>
> To change the language displayed on the user interface and online Help, see the following:
>
> - Configuring Firefox for a Translated Version of the Service
> - Configuring Google Chrome for a Translated Version of the Service
>
> For information to display a translated version of Smart View, see Translation Information in *Oracle Smart View for Office User's Guide*.

Online Help and Guides

Online Help and guides are translated into French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Traditional Chinese, and Simplified Chinese. Smart View documentation is translated into Dutch also.

The translated online help and documentation cover all features up to May 2, 2025, except for *Administering and Working with Oracle Fusion Cloud Enterprise Data Management*, which covers all features up to July 4, 2025.

The English online Help and guides contain up to date information on all features.

Sample Applications and Demos

Sample applications, demos, and data are in English only.

Videos

The overview video closed captions are translated into French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Traditional Chinese, and Simplified Chinese.

Tutorial video closed captions are not translated.

3

Working with Subscriptions

In This Section:

Available Cloud EPM Subscriptions

Oracle Fusion Cloud Enterprise Performance Management provides end-to-end business processes to meet the requirements of most organizations and ensures a connected and agile experience across multiple business processes. The business processes and features available to you depend on the specific Cloud EPM subscription that you purchased.

- The **EPM Standard Subscription** is a powerful, configurable suite of business processes. It is designed primarily for small and mid-sized businesses.
- The **EPM Enterprise Subscription** comprises the full suite of Cloud EPM business processes supporting a comprehensive array of activities. It includes all functionalities of the EPM Standard subscription.

The following table outlines the key features available with Cloud EPM subscriptions.

> **Note**
>
> - AI and GenAI features are available exclusively with EPM Enterprise subscriptions.
> - Intelligent Performance Management (IPM) features are available exclusively with EPM Enterprise subscriptions. For information on the IPM features supported by each business process, see About IPM in *Administering Planning*.
> Exception: AutoPredict is also available with Planning in EPM Standard subscription.
> - Some features available with both EPM Standard and EPM Enterprise subscriptions are not listed in this table. For a comprehensive overview of features related to each business process, refer to the Administrator guides.

Table 3-1 High-level Features Available with Cloud EPM Subscriptions

EPM Standard Subscription	EPM Enterprise Subscription
Planning • Planning Modules – Capital – Financials – Projects – Workforce – Strategic Modeling • One Reporting (ASO) cube and one Input (BSO) cube	**Planning** All EPM Standard subscription features plus: • Application Types: – Custom Planning (with Strategic Modeling support) – FreeForm – Predictive Cash Forecasting – Sales Planning – Strategic Workforce Planning • Multiple Reporting (ASO) and Input (BSO) cubes • Custom Groovy Scripting support • Cloud EPM System Reports within Reports
Account Reconciliation (with Reconciliation Compliance)	**Account Reconciliation** All EPM Standard subscription features plus Transaction Matching
Financial Consolidation and Close • Supplemental Data Management • Financial Consolidation • Support for Complex Ownership Structures • Configurable Consolidation Rules • Equity Pickup • Custom Configurable Calculations and On-demand Rules	**Financial Consolidation and Close** All EPM Standard subscription features plus: • Enterprise Journals • Custom Groovy Scripting support • Cloud EPM System Reports within Reports
Narrative Reporting • Report Packages • Reports	**Narrative Reporting** All EPM Standard subscription features plus : • Report Notes • Cloud EPM System Reports within Reports
	FreeForm
	Enterprise Data Management (with limits on hosted employee and hosted record metrics)

Table 3-1 (Cont.) High-level Features Available with Cloud EPM Subscriptions

EPM Standard Subscription	EPM Enterprise Subscription
	Profitability and Cost Management Application Types: • Enterprise Profitability and Cost Management • Profitability and Cost Management **Tax Reporting** • Tax Provisions • Country by Country Reporting (CbCR) • Pillar Two (Global and Local Top-up Tax) • Supplemental Data Management • Custom Configurable Calculations and On-demand Rules, including Groovy (preview) • Cloud EPM System Reports within Reports

Watch this video to learn more-

 Overview of EPM Standard and EPM Enterprise subscriptions.

Account Reconciliation

The following table outlines key Account Reconciliation features available with EPM Standard and EPM Enterprise subscriptions. It also lists if the feature was available with the legacy subscriptions that are no longer available.

> **Note**
>
> - If a feature is not listed, it is supported in both EPM Standard and EPM Enterprise subscriptions.
> - AI, GenAI, and Intelligent Performance Management (IPM) features, if available, are exclusive to the EPM Enterprise subscription.

Table 3-2 Account Reconciliation Features Availability by Subscription

Features	Legacy subscription	EPM Standard	EPM Enterprise
Reconciliation Compliance	✔	✔	✔
Transaction Matching	✔ Option to purchase		✔

Enterprise Data Management

The Enterprise Data Management business process is only available with the EPM Enterprise subscription.

This offering is different from Oracle Fusion Cloud Enterprise Data Management. See Available Cloud EDM Subscriptions.

Financial Consolidation and Close

The following table outlines key Financial Consolidation and Close features available with EPM Standard and EPM Enterprise subscriptions. It also lists if the feature was available with the legacy subscriptions that are no longer available.

> **Note**
>
> - If a feature is not listed, it is supported in both EPM Standard and EPM Enterprise subscriptions.
> - AI, GenAI, and Intelligent Performance Management (IPM) features, if available, are exclusive to the EPM Enterprise subscription, unless otherwise noted.

Table 3-3 Financial Consolidation and Close Feature Availability by Subscription

Feature	Legacy Subscription	EPM Standard Subscription	EPM Enterprise Subscription
Custom Configurable Calculations and On-demand Rules	✓	✓	✓
Configurable Consolidation Rules	✓	✓	✓
Enterprise Journals	✓		✓
Equity Pickup	✓	✓	✓
Financial Consolidation and Close Management	✓	✓	✓
Groovy Support	✓		✓
Task Manager integrations to automate tasks across Cloud services and on-premises applications	✓		✓
Task Management	✓	✓	✓
Supplemental Data Management	✓	✓	✓
Support for Complex Ownership Structures	✓	✓	✓

FreeForm

The FreeForm business process is only available with the EPM Enterprise subscription.

> **Note**
>
> FreeForm is also available as a Planning application type with the EPM Enterprise subscription.

Narrative Reporting

The following table outlines key Narrative Reporting features available with EPM Standard and EPM Enterprise subscriptions. It also lists if the feature was available with the legacy subscriptions that are no longer available.

> **Note**
>
> - If a feature is not listed, it is supported in both EPM Standard and EPM Enterprise subscriptions.
> - AI, GenAI, and Intelligent Performance Management (IPM) features, if available, are exclusive to the EPM Enterprise subscription, unless otherwise stated.

Table 3-4 Narrative Reporting Feature Availability by Subscription

Features	Legacy Enterprise Performance Reporting Cloud Subscription	EPM Standard Subscription	EPM Enterprise Subscription
Reports	✔	✔	✔
Report Packages	✔	✔	✔
System Reporting			✔

Planning

The following table outlines key Planning application types available with the EPM Standard and EPM Enterprise subscriptions. It also lists if the application type was available with the legacy subscriptions that are no longer available.

> **Note**
>
> - If a feature is not listed, it is supported in both EPM Standard and EPM Enterprise subscriptions.
> - AI, GenAI, and Intelligent Performance Management (IPM) features, if available, are exclusive to the EPM Enterprise subscription, unless otherwise stated.

Table 3-5 Planning Application Types Availability by Subscription

Application Types	Legacy PBCS	Legacy EPBCS	EPM Standard Subscription	EPM Enterprise Subscription
Custom	✔			✔
FreeForm				✔
Modules (Capital, Financials, Projects, Workforce, and Strategic Modeling)		✔	✔	✔
Predictive Cash Forecasting				✔
Sales Planning				✔
Strategic Workforce Planning				✔

Profitability and Cost Management

If you have been using legacy subscriptions for Enterprise Profitability and Cost Management, Profitability and Cost Management, please note that these business processes are now exclusively available with the EPM Enterprise subscription.

Tax Reporting

The following table outlines key Tax Reporting features available with EPM Enterprise subscriptions. It also lists if the features were available with the legacy subscriptions that are no longer available.

> **Note**
>
> - Tax Reporting is not available in the EPM Standard subscription.
> - AI, GenAI, and Intelligent Performance Management (IPM) features, if available, are exclusive to the EPM Enterprise subscription, unless otherwise noted.

Table 3-6 Tax Reporting Feature Availability by Subscription

Feature	Legacy Subscription	EPM Enterprise Subscription
Tax Provision	✓	✓
Interim Tax Provision	✓	✓
IFRS	✓	✓
Country by Country Reporting (CbCR)	✓	✓
Pillar Two (Global and Local Top-up Tax)	✓	✓
Ownership Management	✓	✓
Task Management	✓	✓
Supplemental Data Management	✓	✓
Custom Configurable Calculations and On-demand Rules, including Groovy (preview)	✓	✓

Available Cloud EDM Subscriptions

Oracle Fusion Cloud Enterprise Data Management is a standalone service. See About Cloud EDM. This offering is different from the Enterprise Data Management business process in EPM Enterprise subscription.

Ordering a Subscription

To explore information about Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management, visit the Oracle website. If you're interested in a live demo, simply click the **Request a Demo** button.

When you're ready to make a purchase, reach out to Oracle Sales through one of the following options:

- Click on the  icon and select an option to contact Oracle Sales.
- Scroll to the bottom of the page and click the button under Contact sales to submit your information.

After completing your order, Oracle will send an email to the designated initial contact (the email address you provided when ordering the subscription). This email will outline the steps needed to activate and provision your subscription.

Troubleshooting

See Resolving Order Processing Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Activation Checklist

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management follow an identical activation process. However, some questions should be considered prior to activating your subscription, especially if your cloud ecosystem comprises other complementary Oracle Cloud offerings; for example, Fusion Cloud.

Cloud EPM and Cloud EDM are quite often deployed along with Oracle Fusion Financials Cloud. These subscriptions can be activated into the same Oracle Cloud Account as Oracle Fusion Financials Cloud, and they can either share the same identity domain or use a different one. Also, your test and production environments can be located in different regions, compartments, and identity domains.

The decision to co-locate Cloud EPM and Cloud EDM subscriptions depends on your business needs and other factors such as the geographical spread of users and your organization's tolerance for administrative overheads. For example, you may have a situation where the EPM Cloud users are primarily located in North America while the Cloud EDM users are located in Europe. In such a scenario, you must carefully evaluate whether you want to co-locate subscriptions.

Table 3-7 Activation Options for Cloud EPM and Cloud EDM

	Consideration	Your Response
1	Which subscription did you purchase: EPM Standard, EPM Enterprise, or Cloud EDM	
2	Are you currently using any Oracle Cloud environments such as Cloud EPM, Cloud EDM, or Oracle Fusion Financials Cloud? If so, you already have an Oracle Cloud account. Would you like to add this subscription to share users and security with your existing environments? • If no, create a new Oracle Cloud account. • If yes, activate this subscription into your existing Oracle Cloud account. Then, proceed to item 4. If you are not the Account Administrator for your current Oracle Cloud account, see What if the Existing Oracle Cloud Account was Created by Someone Else?.	
3	If you are creating a new Oracle Cloud account, follow the instruction on the New Cloud Account Information page. See Creating a New Cloud Account. Make your you have all the details of the Cloud Account Administrator, identified the Cloud Account Name, and the default Region in which your account will be provisioned.	

Table 3-7 (Cont.) Activation Options for Cloud EPM and Cloud EDM

	Consideration	Your Response
	This Cloud Account Administrator should have necessary permissions to use the Oracle Cloud Console to create Cloud EPM or Cloud EDM environments and configure security for them.	
4	If you are activating a subscription into an existing Oracle Cloud account, please provide the cloud account name, as well as the username and password of the Cloud Account Administrator. This information is needed to complete the activation process. **Note** If you are not the Account Administrator of the existing Oracle Cloud account, see What if the Existing Oracle Cloud Account was Created by Someone Else?. See Adding Subscription to an Existing Cloud Account for instructions.	

What if the Existing Oracle Cloud Account was Created by Someone Else?

To add an Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management subscription to an existing Oracle Cloud Account, you must be an Oracle Cloud Account Administrator.

The user whose information was used to create the Oracle Cloud account, by default, is defined as the Account Administrator. This user can use the Oracle Cloud Console to create other users and grant them administrator privileges, making them Oracle Cloud Account Administrators by adding them to the Administrators group.

To create an Oracle Cloud Account Administrator:

1. Sign into the Oracle Cloud Console as the Oracle Cloud Account Administrator. See Accessing Oracle Cloud Console.
2. Within the default domain, create a user if necessary and assign the user to the Administrators group. See Granting Service Administrators Access to the Oracle Cloud Console.

Note

If you are using an existing user account, make sure that it is assigned to the Administrators group.

Activating Cloud EPM Subscription

Related Topics

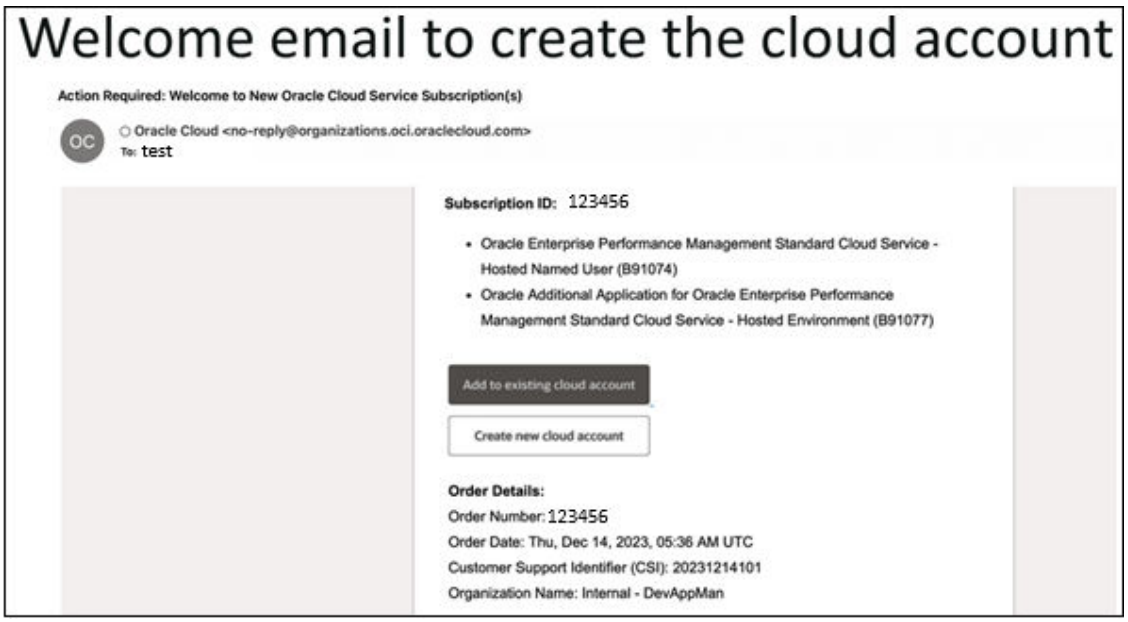
- The Subscription Activation Email

- Creating a New Cloud Account
- Adding Subscription to an Existing Cloud Account

The Subscription Activation Email

> **Note**
>
> Before activating the subscription, review the important considerations listed in the Activation Checklist.

When you purchase a new Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management subscription (see Ordering a Subscription), Oracle sends an email outlining the activation steps.



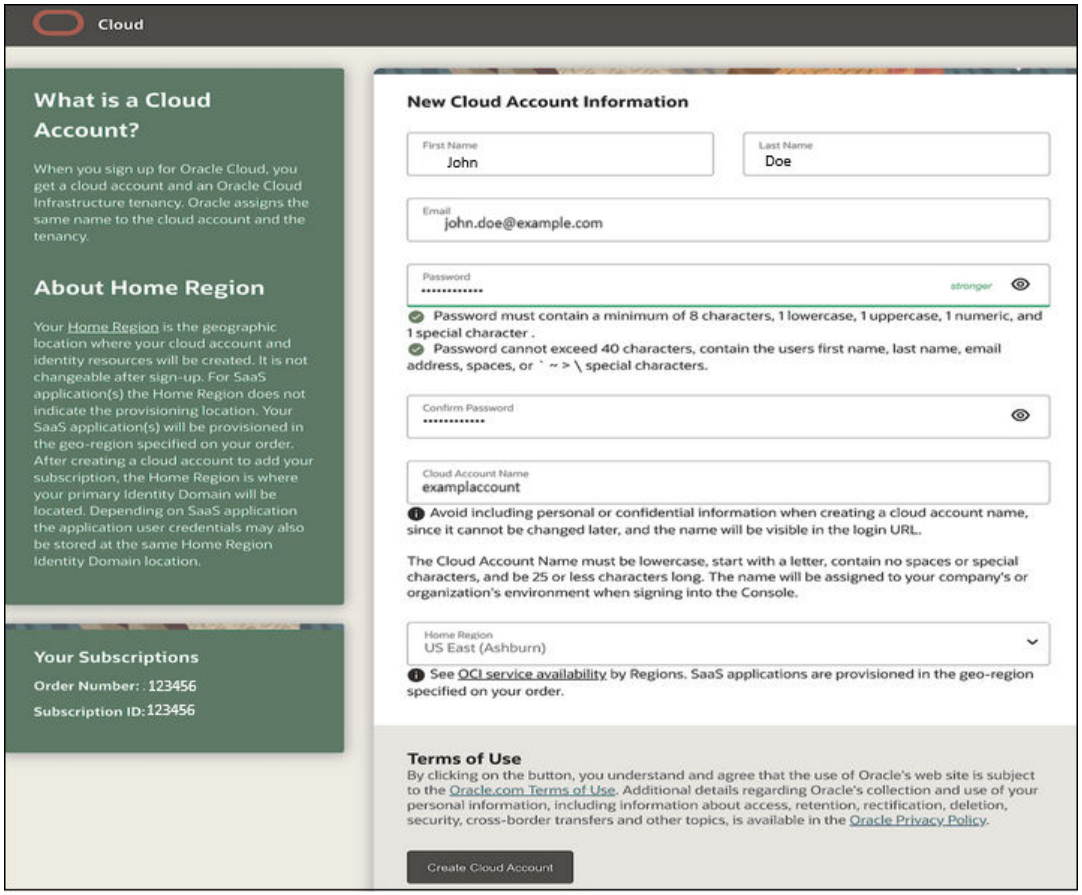
You can choose to create a new account or add the subscription to an existing cloud account to complete the activation. See:

- Creating a New Cloud Account
- Adding Subscription to an Existing Cloud Account

Creating a New Cloud Account

To create an Oracle Cloud account and activate your subscription:

1. Click **Create new cloud account** on the activation email. See The Subscription Activation Email.
   The **New Cloud Account Information** form opens in a browser.



2. Enter your **First Name**, **Last Name**, and **Email Address**. The email address is also the user name for signing in to the Oracle Cloud account. The person you specify here will be the tenancy administrator and will be able to perform all operations within this tenancy.
3. Enter a **Password** and confirmation.
4. Enter a **Cloud Account Name** which is your tenancy name. This value, which cannot be changed later, is visible in your login URLs.
5. Select a **Home Region**. This is the region in which your cloud account will be provisioned. This is the region where IAM instance will be located and thus, your user information is located.

> **Note**
>
> It is important to choose your home region carefully, as it cannot be changed once your cloud account is created. You can provision your cloud account in any region supported by OCI for your realm. For a list of available regions, see Geographical Regions and Identifiers in the *Cloud Operations Guide*. Take into consideration any data residency requirements while selecting the home region.

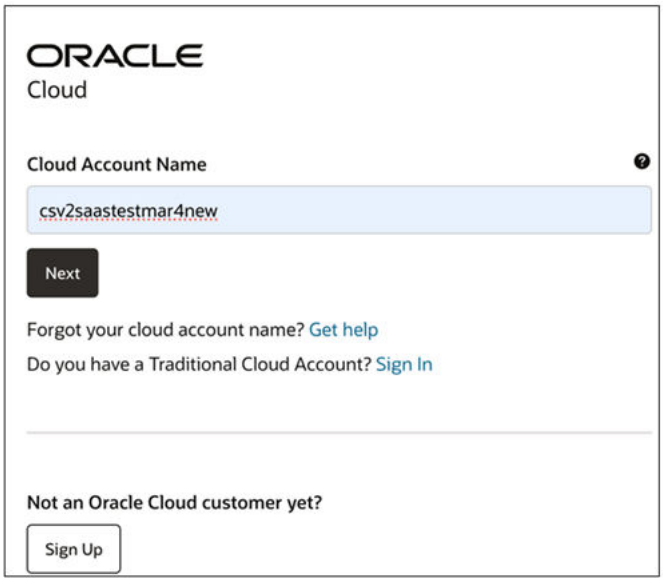
6. Read the **Terms of Use**.
7. Click **Create Cloud Account**. When your new tenancy is created, you will receive an email with detailed information.
8. Click **Sign In** in the email to sign in for the first time with the credentials you set up.

9. Sign In and access the console. See Getting Started with Oracle Cloud Console.

Adding Subscription to an Existing Cloud Account

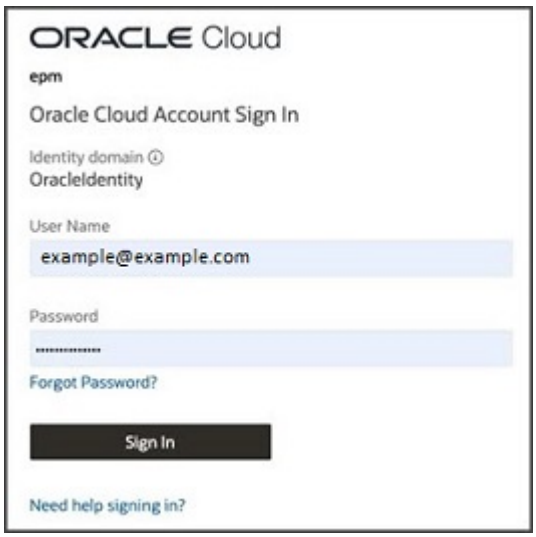
Once a subscription is added to a cloud account, it cannot be undone. If you are an existing Oracle Cloud customer and wish to activate the subscription in an existing cloud account, follow these steps:

1. Click **Add to existing cloud account** in the activation email. See The Subscription Activation Email.
2. For **Tenancy**, enter the name of the existing cloud account, and then click **Continue**.



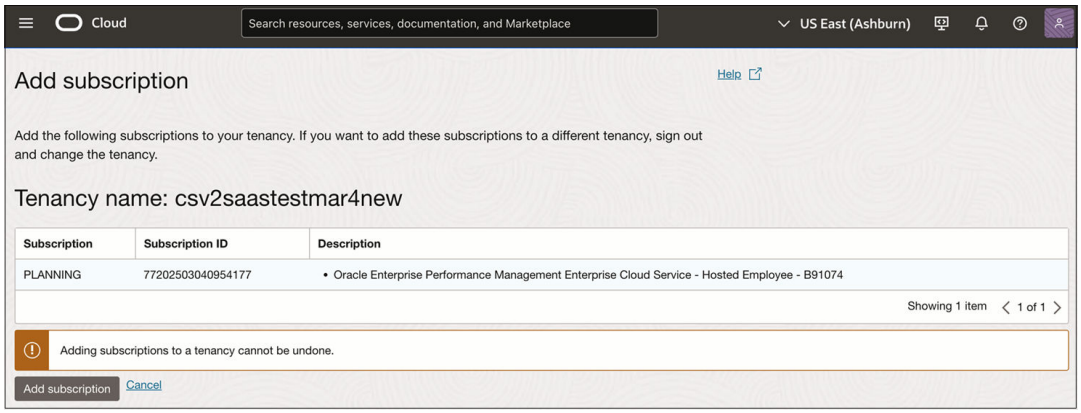
The Oracle Cloud Account Sign In page opens.

3. Enter your user name and password, and then click **Sign In**.



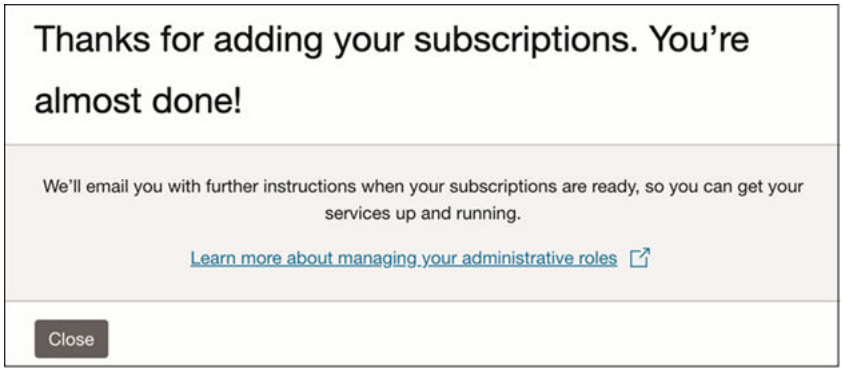
The Add Subscription page is displayed, where you can add the new subscription to your cloud account. The page indicates the subscription name, ID, and description.

4. Click **Add subscription**.



The subscription is added to the tenancy.

5. A confirmation message is displayed.



Activating Cloud EDM Subscription

Oracle Enterprise Data Management is available in two forms:

- **Enterprise Data Management business process**: Available with the EPM Enterprise subscription. To activate, see Activating Cloud EPM Subscription
- **Oracle Fusion Cloud Enterprise Data Management:** Available as a standalone cloud service subscription. For more details, see About Cloud EDM.

> **Note**
>
> The activation email that Oracle sends may refer to Oracle Fusion Cloud Enterprise Performance Management instead of Cloud EDM.

To activate both forms of Oracle Enterprise Data Management, these deployment scenarios are available:

- Activate a new Enterprise Data Management Business Process into a new cloud account. See Creating a New Cloud Account.
- If you already have other Cloud EPM business processes:
  - Activate the Enterprise Data Management business process or Cloud EDM into an existing cloud account, allowing you to share the identity domain (users and groups) with other business processes. See Adding Subscription to an Existing Cloud Account.
  - Activate Enterprise Data Management business process or Cloud EDM into a new cloud account, which will not allow sharing the identity domain with existing EPM Cloud business processes. See Creating a New Cloud Account.
- If you only have Cloud EDM subscription, activate into a new cloud account. See Creating a New Cloud Account.
- If you have Oracle Fusion Financials Cloud, activate the Enterprise Data Management business process or Cloud EDM based on one of the above scenarios.

Getting Started with Oracle Cloud Console

For OC1 environments migrated to the Oracle Cloud Console, Service Administrators have been already been added to the *planning_Console_Upgrade_Service_Admin_Group* and the *Planning_Console_Upgrade_Service_Admin_Group_Policy* has been applied to this group, granting them access to the Oracle Cloud Console.

> **Note**
>
> The group and policy names may differ if your subscription is not an EPM Enterprise or EPM Standard subscription. For example, they might be named *arcs_Console_Upgrade_Service_Admin_Group* and *arcs_Console_Upgrade_Service_Admin_Group_Policy* respectively.

For newly created accounts as well as migrated environments in restricted realms (i.e., OC2, OC3, OC4, and OC19), only Account Administrators have default access to the Oracle Cloud Console. Service Administrators of individual environments must be explicitly assigned the

necessary policies to view those environments in Oracle Cloud Console. See Granting Service Administrators Access to the Oracle Cloud Console.

In This Section:

Enabling Multifactor Authentication

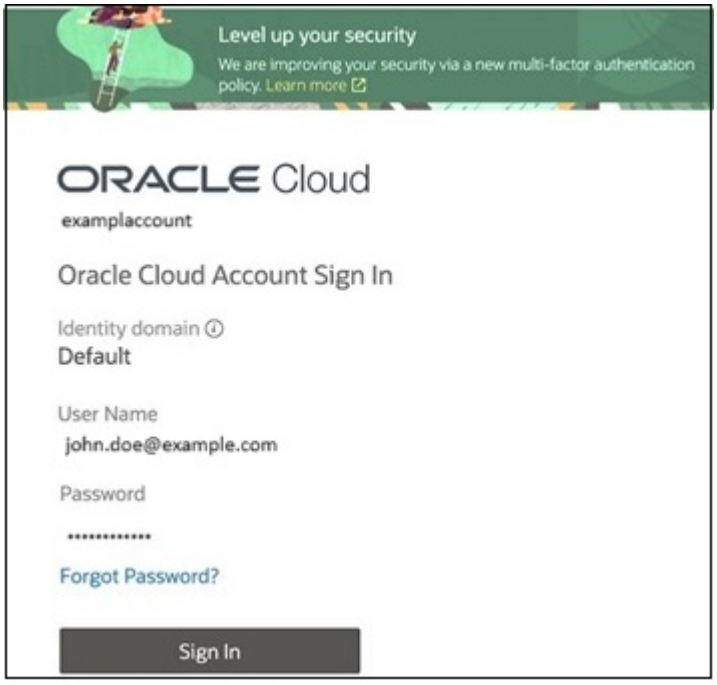
Access to the Oracle Cloud Console requires you to use Multifactor Authentication (MFA).

When MFA is enabled, you must first enter the username and password—this serves as the first factor (something you know). You will then be prompted to provide a verification code from a registered MFA device, which is the second factor (something you have). This combination of factors adds an extra layer of security to confirm the identity during sign-in.

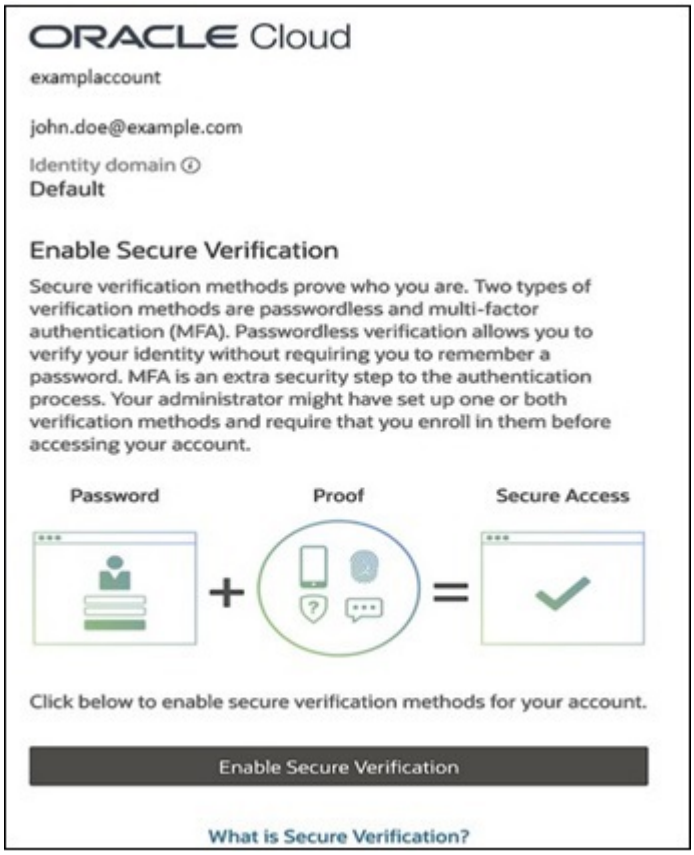
Before enabling MFA, ensure you have a supported authenticator app installed on your mobile device. Examples include Oracle Mobile Authenticator and Google Authenticator. You'll use the app to register your device and generate a time-based one-time passcode (TOTP) each time you sign in.

To enable MFA:

1. Using a browser, go to `https://www.oracle.com/cloud/sign-in.html`.
2. Sign in to your cloud account.



3. Click **Enable Secure Verification**.



4. Select the MFA option for secure verification. Usually users select the Mobile App option.
5. Scan the QR code.

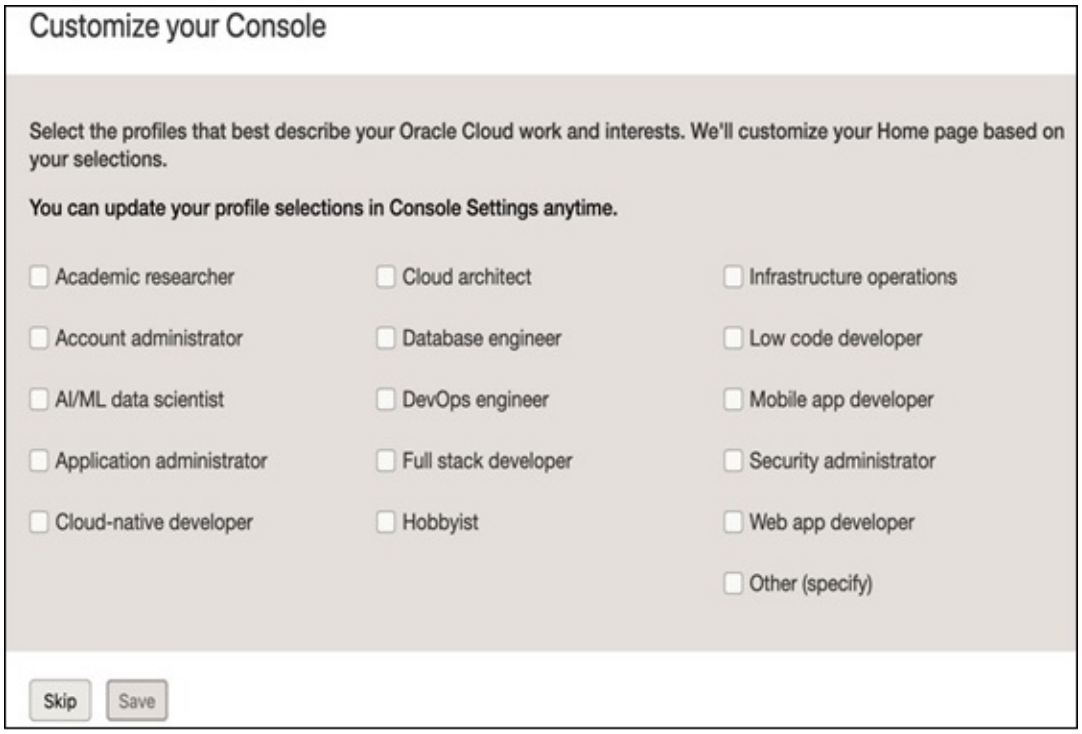
Your mobile device is now registered with the IAM service and your account is enabled for MFA. When you sign into Oracle Cloud Console, it will now send a notification to your mobile device. Open the notification in the app, and then tap **Allow** to continue.

Accessing Oracle Cloud Console

To access the Oracle Cloud Console:

1. Using a browser, go to `https://www.oracle.com/cloud/sign-in.html`. Sign in using Multi-Factor Authentication (MFA). See Enabling Multifactor Authentication.
2. In the Welcome to Oracle Applications screen, click **Begin Tour** to proceed to the guided tour of Oracle Cloud Console. You can also click **I'll explore on my own** and skip the tour.

3. Optionally, customize the console by selecting your profile. Use this opportunity to select the profiles that best describe your Oracle Cloud work and interests, then click **Save**. The Console home page is then tailored to your choices. For more information, see Using the Oracle Cloud Console.



Subscribing to and Replicating Regions

A **region** is a geographical location where your Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment is hosted. Your **Home region** is the primary location your cloud account and identity data are stored and managed. By default, you can only view environments within your home region.

To view and work with environments in a region other than your home region, you must first subscribe to them. For example, if your home region is *us-phoenix-1*, you can only view and create environments in *us-phoenix-1*. To view and create environments in *us-ashburn-1*, you must first subscribe to *us-ashburn-1*.

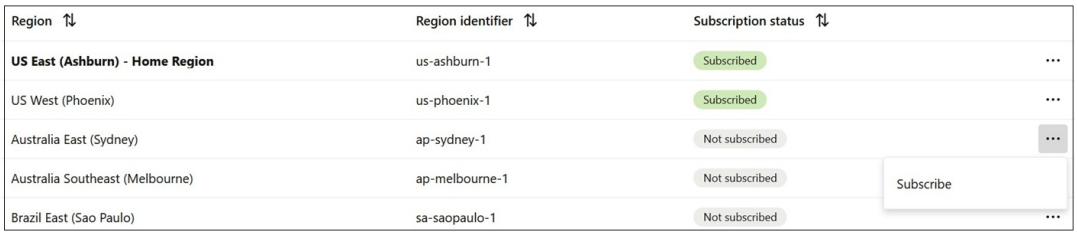
To ensure seamless access and avoid console errors, **identity data from your home region must be replicated** to every region you are subscribed to. While the *Default* identity domain is replicated automatically, other domains require manual replication.

For a complete list of available regions, see OCI (Gen 2) Geographical Regions and Identifiers in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Subscribing to a New Region

1. From the Application home page, open the **Regions** menu in the top navigation bar. A list of regions available to your cloud account is displayed.

2. Select **Manage regions**.
3. Locate the region you want to subscribe to. Click the **ellipses (…)** next to the target region, then select **Subscribe**.

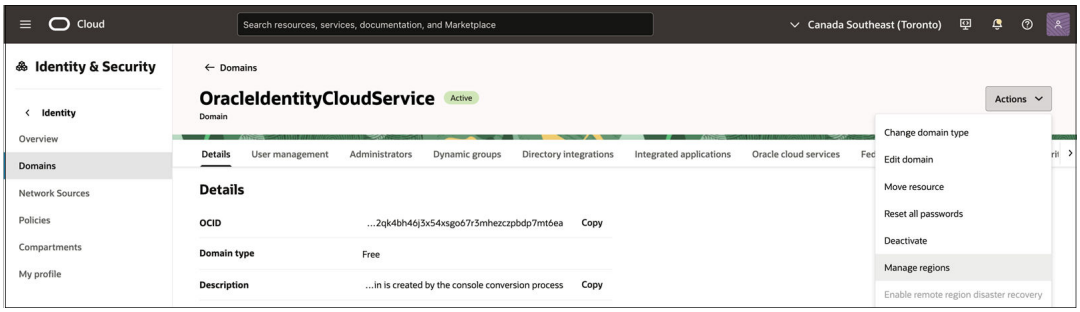


> **Note**
>
> It may take several minutes to activate your cloud account in the new region.

Remember, your identities are global, so when the subscription becomes active, all your existing policies are enforced in the new region. You cannot unsubscribe from a region.

Replicating to a Subscribed Region

1. Open the **Navigation** menu, search for "Identity," and select **Domains**.
2. On the Domains page, select the domain you want to replicate to open the domain details.
3. Click **Actions**, then select **Manage regions** to open the Manage regions page.



4. Locate the target regions in the list. For each target region, click the **ellipses (...)** next to the region, and select **Enable replication**.

The replication process may take upto 60 minutes, depending upon the size and configuration of your identity setup.

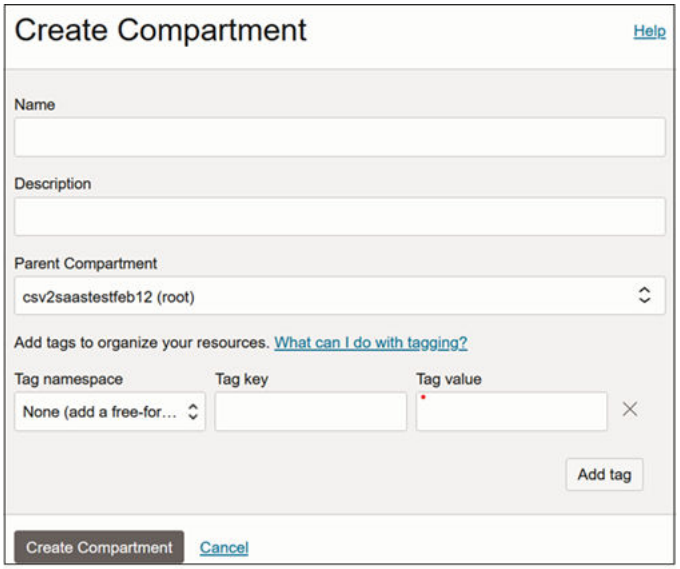
Creating a Compartment

The Oracle Cloud Console is designed to display your resources by *compartment* within the current region. When you work with your resources in the Oracle Cloud Console, you must choose which compartment to work in from a list on the page. That list is filtered to show only the compartments in the tenancy that you have permission to access. If you're an administrator, you'll have permission to view all compartments and work with any compartment's resources, but if you're a user with limited access, you probably won't.

You can create compartments in your Oracle cloud account, across regions, to organize your environments. When you create a compartment, it is available in every region that your tenancy is subscribed to.

To create a compartment:

1. Sign in to the Oracle Cloud Console.
2. Go to the **Navigation** menu, search for *Identity*, select **Compartments**.
   A list of the compartments you have access to in the tenancy is displayed.
3. To create the compartment in the tenancy (root compartment) select **Create Compartment**. Otherwise, select through the hierarchy of compartments until you reach the detail page of the compartment in which you want to create the compartment. Then, on the details page, select **Create Compartment**.



4. Enter the name, description, parent compartment, and tags.
5. Click **Create Compartment**.

Authenticating and Authorizing

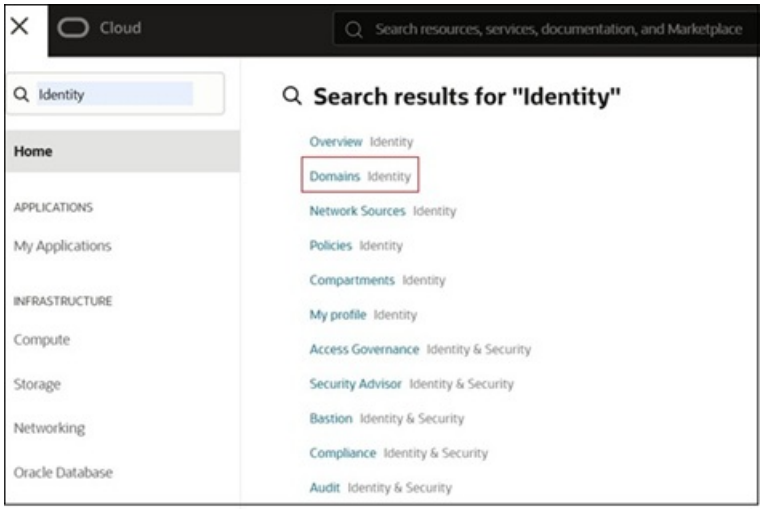
Related Topics

- Accessing the IAM Interface
- Creating an Identity Domain
- Adding Identity Domain Administrators

Accessing the IAM Interface

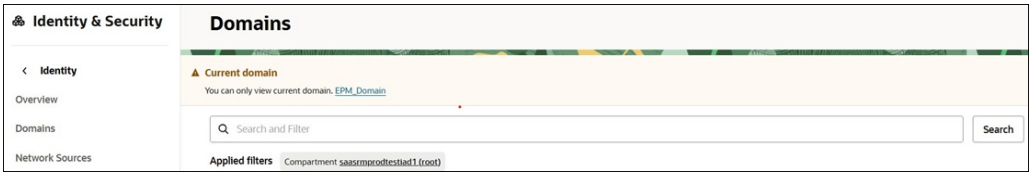
To access the Identity and Access Management (IAM) interface for a specific identity domain:

1. Sign in to the Oracle Cloud Console as an Account Administrator or Identity Domain Administrator.
2. From the **Navigation** menu, search for "Identity," and select **Domains**.



3. On the **Domains** page:

   a. To access your current domain, click the domain link on top under Current domain message.



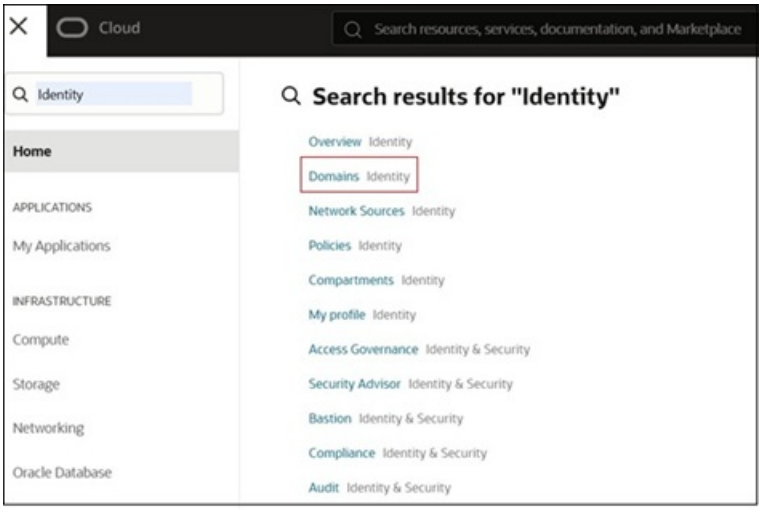
   b. To access a different domain, search for and select it from the list. You will be directed to the **Details** tab of the selected domain.

Creating an Identity Domain

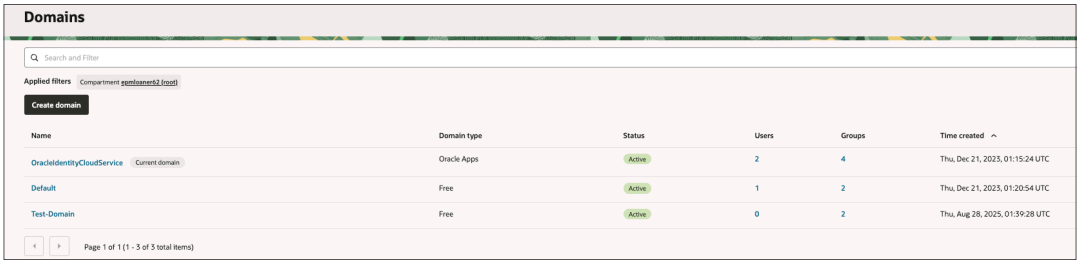
You can create more than one domain in the IAM Interface. Your test and production environments can be located in different identity domains. To create an identity domain, administrators need to know which identity domain type they want to create, in which compartment to create it, and the new identity domain administrator's sign-in credentials, if needed.

To create an identity domain:

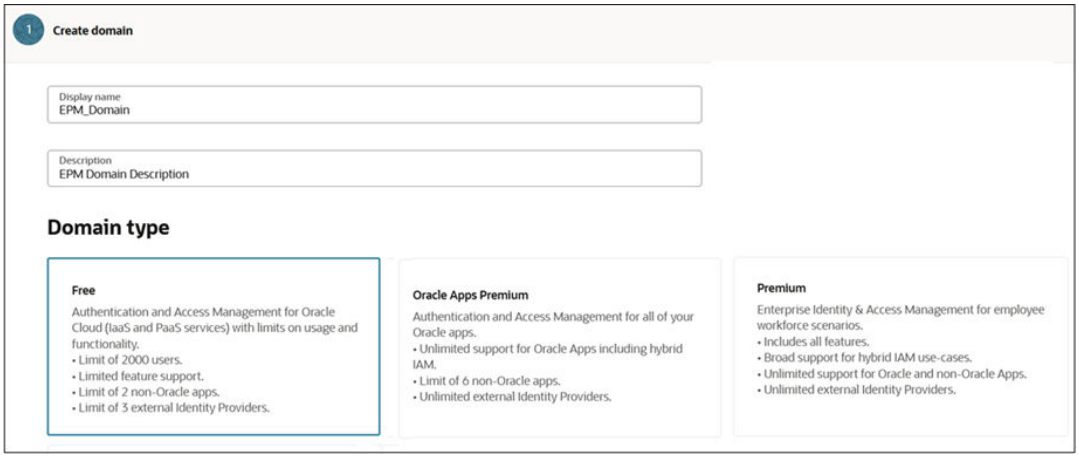
1. From the **Navigation** menu, search for "Identity," and select **Domains**.



2. On the **Domains** page, click **Create domain**.

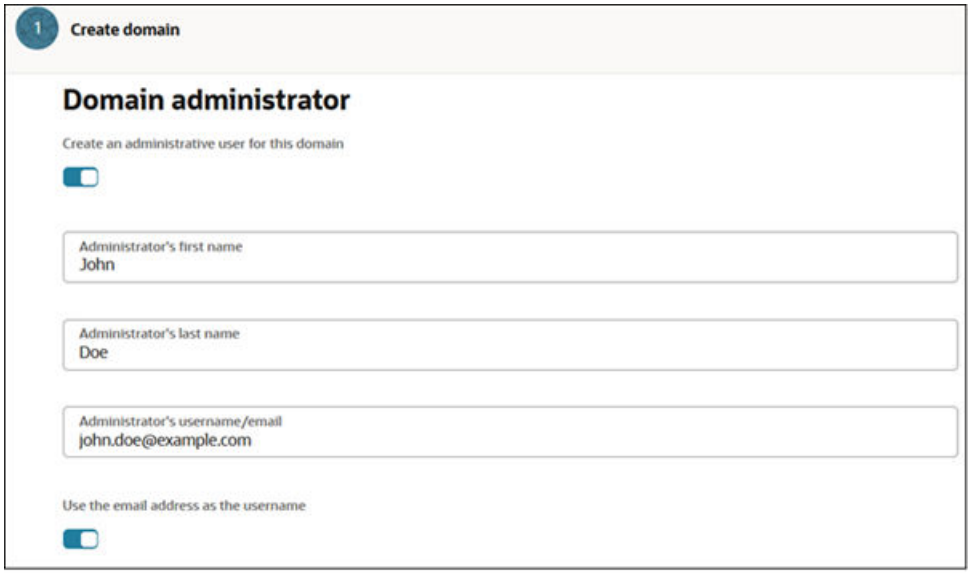


3. On the **Create domain** page, enter a display name and description. Choose **Free** for the domain type. When you later create an environment within this domain, its domain type will be changed to **Oracle Apps**.



4. Enter the details of the user who you want to administer this identity domain.

> **Note**
>
> Granting users or groups the Identity Domain Administrator role for domains other than the default domain grants them full administrator permissions to only that domain (not to the tenancy). At least one administrator for the identity domain must be granted the Identity Domain Administrator role directly. This is in addition to any Identity Domain Administrator roles granted by group membership.



5. Verify that the correct compartment is selected.
6. To add tagging, click **Add tag** and enter the tagging details.

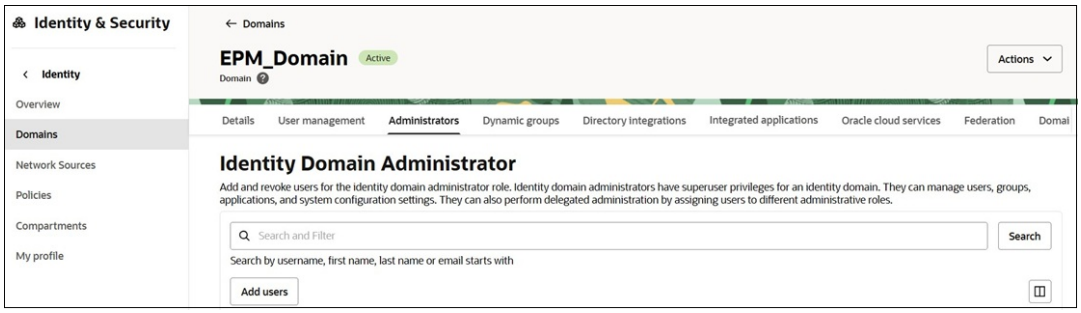
7. Under **Remote region disaster recovery**, click **Enable remote region disaster recovery**. You must be subscribed to the paired region to enable remote region disaster recovery. For example, if your home region is US East (Ashburn), then you must be subscribed to US West (Phoenix). For more information, see Disaster Recovery Region Pairings.
8. Under **Review and Create**, click **Create**.

Adding Identity Domain Administrators

The Cloud Account Administrator (Tenancy Administrator) can delegate setup tasks by creating Identity Domain Administrators.

To create Identity Domain Administrators:

1. Access your domain on the IAM Interface. See Accessing the IAM Interface.
2. Click **Administrators** tab.



3. In **Identity Domain Administrator**, click **Add users**.
4. In **Add Identity domain administrator**, select the users to be assign the Identity Domain Administrator role, and then click **Add users**.
   The new users added are now listed as Identity Domain Administrators.

Setting Up a Cloud EPM or Cloud EDM Environment

With your subscription, you receive two environments: test and production. When creating an environment, you'll designate it as a test or production environment. During setup, you'll also specify an environment name, which will be included in the URLs used to access your environments. Once created, the environment name cannot be changed, so it's important to select the name carefully.

To create an environment, you must have the Account Administrator role.

If you're not creating your environment using the default options, make sure to do the following before you begin:

- Subscribe to a different region if you are not setting up the environment in the home region. See Subscribing to and Replicating Regions.
- Create a new compartment. See Creating a Compartment.
- Create a new identity domain if you would like to segment users, improve security, and simplify the process of managing Identity and Access Management use cases. See Creating an Identity Domain.

Your test and production environments can be located in different regions, compartments, and identity domains.

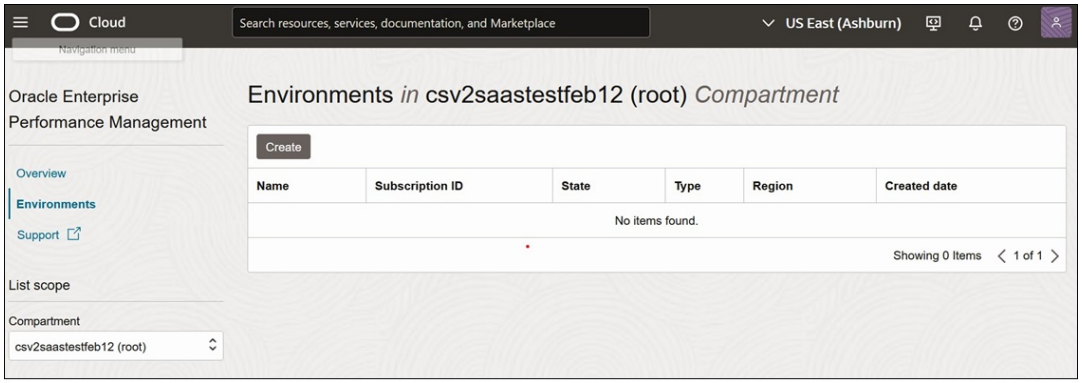
Creating an Environment

Before creating an environment in a region other than the home region of your cloud account, you must first subscribe to that region. For more information, see Subscribing to and Replicating Regions.

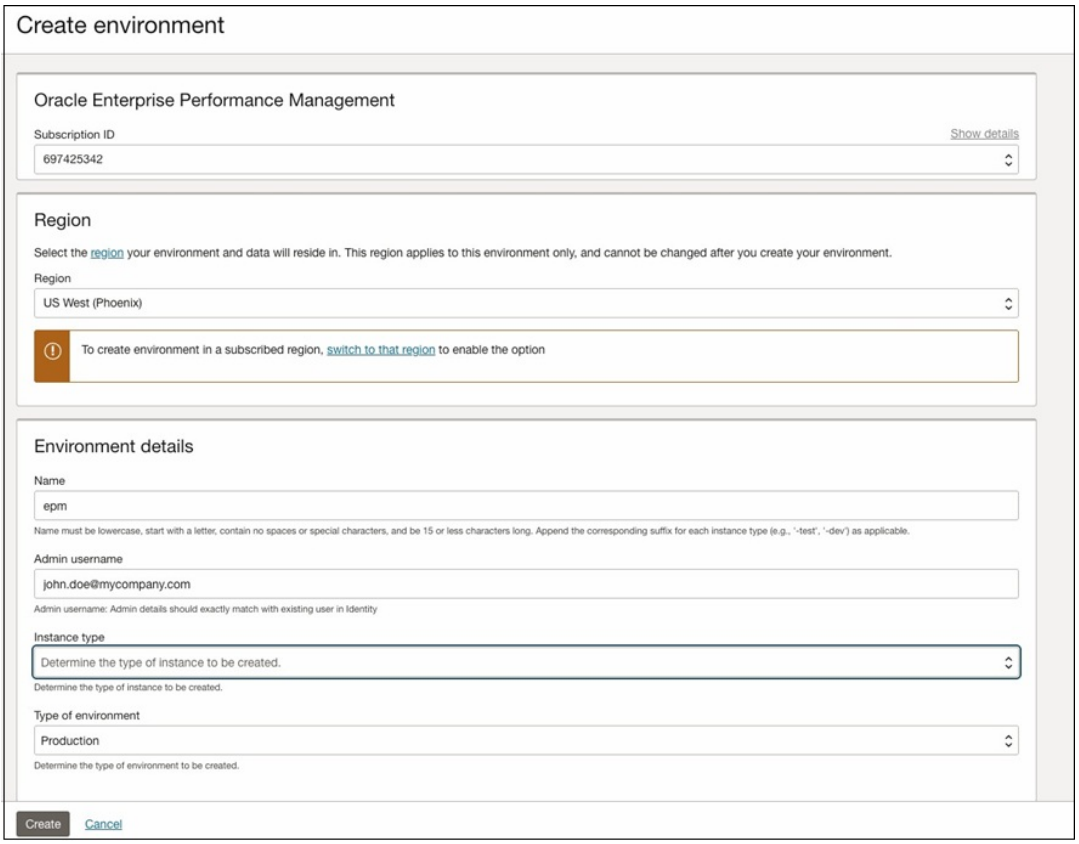
To create a new environment:

1. From the **Navigation** menu, select **My Applications**, click **Oracle Enterprise Performance Management**.
2. Select **Environments** on the left pane.

3. Click **Create** to create a new environment.



4. On **Create environment**, select a region to which you have already subscribed. If you haven't subscribed to any additional regions, your home region will be displayed by default. You can create production and test environments in different regions.



5. Under **Environment details**, provide the following information:

   a. Enter the **Name** of the environment. Name must be lowercase, start with a letter, contain no spaces or special characters, and be 20 or less characters long. This name can't be changed later.

> **Note**
>
> You can create the test and production environments in any order, but they must be in equal numbers. For example, if five pairs are allowed, you cannot create six production and four test environments; you must create five production and five test environments. Additionally, the test environment name must match the production name with a *-test* suffix. For example, the environment names could be *epm* and *epm-test*.

b. Select the **Instance type**. The instance types available to you are determined by the subscription you purchased.

c. To assign a user as a Service Administrator, add the **Admin username**.

> **Note**
>
> - This user must already be created in IAM.
> - You can provide different email IDs for the production and test environments.

d. Click and select **Type of environment**.

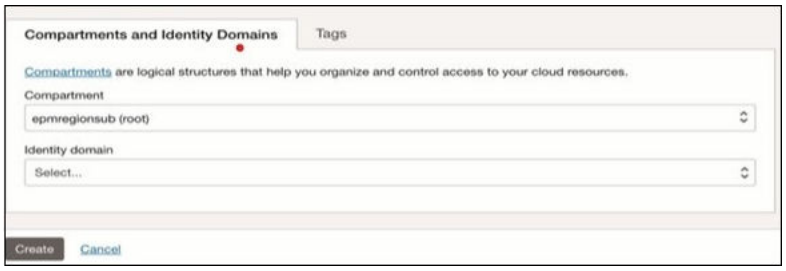
6. Under **Compartment and Identity domains**, provide the following information:

a. Select **Compartments** to select a different compartment if you'd like to create the environment in one other than the default. If no compartments have been created in your tenancy, only the root compartment will be available.

> **Note**
>
> Compartments without an associated domain cannot be selected.

b. Select **Identity Domain** if you would like to segment users, improve security, and simplify the process of managing Identity and Access Management use cases. You can create production and test environments in different domains.

> **Note**
>
> By default, the **OracleIdentityCloudService** domain will be selected if it is available; otherwise, the **Default** domain will be used. You can still choose a different domain from the dropdown as needed.



7. Click **Create** to create the environment.
   You can track the progress of your environment creation by viewing the status of the work request. Initially, the state is **Creating**.

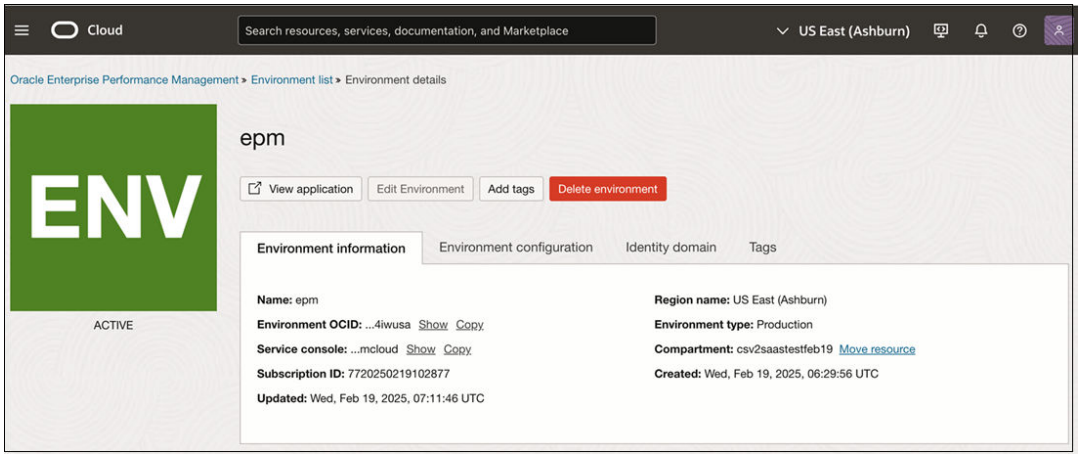
Deleting an Environment

When you delete an environment (either test or production), all data within that environment will also be deleted. Additionally, the URLs for the current environments will become invalid. Be sure to back up any important data and snapshots before deleting an environment. Once the quota becomes available again, you can recreate the environment with your desired new name.

> **Note**
>
> The Account Administrator can delegate setup and configuration activities by creating Identity Domain Administrators and Service Administrators in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

To delete an environment:

1. From the **Navigation** menu, select **My Applications**, click **Oracle Enterprise Performance Management**.
2. From the Environment list, select the environment you wish to delete.
3. Click **Delete environment**.



Renaming or Relocating an Environment

During environment setup, you select a cloud account, specify an environment name, and choose the region where the environment will be created. These details are included in the URL used to access the environment. If you want to change any of the cloud account, environment name, or region, then a new environment must be created, and the existing

environment must be cloned to it. The specific steps vary slightly depending on what you're changing.

Changing the Cloud Account Name

1. Work with your Sales team to submit a new order.
2. Create a new cloud account once you receive the activation email. See Creating a New Cloud Account.
3. Recreate all environments that need to use the new cloud account. See Creating an Environment.
4. Clone the existing environments to the new ones. See Cloning Cloud EPM Environments in *Administering Migration for Oracle Enterprise Performance Management Cloud*.
5. Once cloning is successful, terminate the old environments. See Deleting an Environment.

Changing the Environment Name or Region

1. If you don't have enough quota available to create new environments, work with your Sales team to submit a new order.
2. Once you receive the activation email, use your existing cloud account. Adding Subscription to an Existing Cloud Account
3. Recreate the environments with the desired environment name or region. See Creating an Environment.
4. Clone the existing environments to the new ones. See Cloning Cloud EPM Environments in *Administering Migration for Oracle Enterprise Performance Management Cloud*.
5. Once cloning is successful, terminate the old environments. See Deleting an Environment.

> **Note**
>
> - In both cases, the URLs used to access the environments will change.
> - If you perform these actions on environments created with **Oracle-Managed OCI Migration**, your existing Classic URLs will no longer persist.

Granting Service Administrators Access to the Oracle Cloud Console

By default, the Oracle Cloud Console is accessible only to Cloud Account Administrators and Identity Domain Administrators. Service Administrators of individual environments must be assigned the appropriate policies to access and view those environments in the Oracle Cloud Console.

For newly created environments, Identity Domain Administrators can assign these policies by adding Service Administrators to groups that are linked to specific policies. You can create multiple groups, each with its own policy, and assign users accordingly. This approach allows for granular control over the actions each group of users can perform.

> **Note**
>
> For environments migrated from My Services to the Oracle Cloud Console, Service Administrators have already been added to the *planning_Console_Upgrade_Service_Admin_Group* and the *Planning_Console_Upgrade_Service_Admin_Group_Policy* has been applied to this group.
> It is important that this group and policy are not deleted, as this would cause Service Administrators to lose access to the Oracle Cloud Console.

To provide Service Administrators with permissions to access environments in Oracle Cloud Console :

1. Access your domain on the IAM Interface. See Accessing the IAM Interface.
2. (Optional) If needed, create the users and groups to whom you want to assign policies. See:
   a. Creating User
   b. Creating IDCS Groups
3. Create a policy for the selected group of users assigned as Service Administrators. See Creating Policies for Users and Groups.
   In **Policy Builder**, enter the following policy statements:

   > **Note**
   >
   > Be sure to replace *GROUP_NAME* with the name of the group to which you want to apply the policy

```
Allow group <identity-domain-name>/GROUP_NAME to manage epm-planning-
environment-family in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read epm-planning-
environment-family in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
subscriptions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
assigned-subscriptions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
subscription-regions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read app-listing-
environments in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read metrics in tenancy
Allow group <identity-domain-name>/GROUP_NAME to inspect domains in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read announcements in
tenancy
```

4

Migrating to Cloud EPM and Cloud EDM

In This Section:

Migrating to Cloud EPM

Migration enables you to perform lifecycle management activities for all Oracle Fusion Cloud Enterprise Performance Management business processes other than Narrative Reporting. Migration is available separately for test and production environments.

Every day, during the operational maintenance of the environment, Oracle backs up the content of the environment to create a maintenance snapshot of existing artifacts, setup data, and Data Management staging table data. This snapshot then can be used to migrate content to another environment. See Overview of the Maintenance Snapshot.

Migration Paths for Legacy Snapshots

A legacy snapshot is a snapshot taken from an environment that does not belong to either the EPM Standard or EPM Enterprise subscription.

Essbase in Legacy Environment

> **Note**
>
> You cannot enable the use of Hybrid BSO cubes in legacy Planning and Budgeting cloud environments. See About Essbase in Cloud EPM.

Table 4-1 Migration Scenarios for Legacy Snapshots

Legacy Snapshot Source	Available Migration Paths	Unavailable Migration Paths
Planning and Budgeting Cloud	• EPM Enterprise - Custom • Legacy Planning and Budgeting Cloud	• EPM Enterprise Planning Modules, FreeForm • EPM Standard - Planning
Planning and Budgeting Cloud with Plus One option	• EPM Enterprise - Planning Modules • Legacy Planning and Budgeting Cloud with Plus One option	• EPM Standard • EPM Enterprise, FreeForm, Custom • Legacy Planning and Budgeting Cloud

Table 4-1 (Cont.) Migration Scenarios for Legacy Snapshots

Legacy Snapshot Source	Available Migration Paths	Unavailable Migration Paths
Enterprise Planning and Budgeting Cloud	• Legacy Enterprise Planning and Budgeting Cloud • EPM Enterprise - Planning Modules	• EPM Standard • EPM Enterprise - Custom, FreeForm
• On-Premises 11.2.x Planning * • On-Premises 11.1.2.4 Planning • On-Premises 11.1.2.3 Planning	• EPM Enterprise - Custom • Legacy Planning and Budgeting Cloud	• EPM Standard • EPM Enterprise - Planning Modules, FreeForm • Legacy Planning and Budgeting Cloud
Financial Consolidation and Close without Extended Dimensionality	Legacy Financial Consolidation and Close environments without Extended Dimensionality	• EPM Standard • EPM Enterprise
Financial Consolidation and Close with Extended Dimensionality	• EPM Enterprise • Legacy Financial Consolidation and Close with Extended Dimensionality	• EPM Standard • Legacy Financial Consolidation and Close environments without Extended Dimensionality
On-Premises 11.1.2.4 Oracle Hyperion Financial Management (see About Financial Management Migration)	• EPM Standard • EPM Enterprise • Legacy Financial Consolidation and Close environments	
Tax Reporting Cloud	• EPM Enterprise - Tax Reporting • Legacy Tax Reporting Cloud	EPM Standard
Account Reconciliation	• EPM Enterprise - Account Reconciliation • Legacy Account Reconciliation environments	EPM Standard
On-Premises 11.1.2.4.250 (and later) Oracle Hyperion Financial Close Management	• EPM Standard - Account Reconciliation • EPM Enterprise - Account Reconciliation • Legacy Account Reconciliation environments	
On-Premises 11.1.2.4.002 Oracle Hyperion Strategic Finance (see About Strategic Finance Migration)	• EPM Enterprise - Planning Modules • EPM Enterprise - Custom • EPM Standard	• Legacy Planning and Budgeting Cloud • Legacy Enterprise Planning and Budgeting Cloud • EPM Enterprise - FreeForm

Table 4-1 (Cont.) Migration Scenarios for Legacy Snapshots

Legacy Snapshot Source	Available Migration Paths	Unavailable Migration Paths
Profitability and Cost Management	• EPM Enterprise - Enterprise Profitability and Cost Management • EPM Enterprise - Profitability and Cost Management • Legacy Profitability and Cost Management	EPM Standard
On-Premises 11.1.2.4 Profitability and Cost Management	EPM Enterprise - Profitability and Cost Management	• EPM Standard • Legacy Profitability and Cost Management • EPM Enterprise - Enterprise Profitability and Cost Management
On-Premises 11.1.2.4 Management Ledger Profitability and Cost Management	EPM Enterprise - Enterprise Profitability and Cost Management	EPM Standard
Enterprise Performance Reporting Cloud	• EPM Standard - Narrative Reporting • EPM Enterprise - Narrative Reporting • Legacy Narrative Reporting	
Enterprise Data Management Cloud	• Oracle Enterprise Data Management Cloud • EPM Enterprise - Enterprise Data Management • Legacy Enterprise Data Management	EPM Standard

* On-Premises 11.2.x Planning that uses Oracle Essbase 21c cannot be migrated to Oracle Fusion Cloud Enterprise Performance Management.

About Financial Management Migration

You use the EPM Cloud Migration Accelerator to migrate On-premises 11.1.2.4 Financial Management to Cloud EPM. For detailed instructions, see "Migrate Financial Management to Financial Consolidation and Close" in *Administering Migration*.

About Strategic Finance Migration

See these information sources.

- For detailed migration instructions, see "Migrate Strategic Finance to Strategic Modeling" in *Administering Migration*.
- For instructions to enable Strategic Finance in custom Planning and Planning Modules applications, see Setting up Strategic Modeling in *Administering Planning* .

About Data Relationship Management Migration

You can migrate On-Premises 11.1.2.4.330 or newer Oracle Data Relationship Management to the standalone Oracle Fusion Cloud Enterprise Data Management or to EPM Enterprise - Enterprise Data Management business process.

Limits apply to the number of records in some Enterprise Data Management environments. See About Cloud EDM for an explanation of available Enterprise Data Management subscriptions.

See these information sources:

- For a summary of migration steps, see "Migrate Data Relationship Management to Oracle Enterprise Data Management Cloud" in *Administering Migration*.
- For detailed migration instructions, see Migrating Enterprise Data from Data Relationship Management to Oracle Enterprise Data Management Cloud in *Administering and Working with Oracle Fusion Cloud Enterprise Data Management*.

Migration Paths for EPM Standard and EPM Enterprise Subscription Snapshots

All environments that use Oracle Essbase can support Hybrid BSO Cubes. By default, Financial Consolidation and Close, Custom Planning, Planning Modules, and FreeForm applications use Hybrid BSO cubes. See About Essbase in Cloud EPM.

Table 4-2 Migration scenarios for EPM Standard and EPM Enterprise snapshots

Snapshot Source	Available Migration Paths	Unavailable Migration Paths
EPM Standard - Planning	• EPM Standard - Planning • EPM Enterprise - Planning Modules	• EPM Enterprise - FreeForm, Custom • Legacy Planning and Budgeting Cloud • Legacy Enterprise Planning and Budgeting Cloud
EPM Enterprise - Custom Planning	EPM Enterprise - Custom Planning	• EPM Standard • EPM Enterprise - FreeForm, Planning Modules • Legacy environments
EPM Enterprise - Planning Modules	EPM Enterprise - Planning Modules	• EPM Standard • EPM Enterprise - Custom, FreeForm • Legacy environments
EPM Enterprise - FreeForm	EPM Enterprise - FreeForm	• EPM Standard • EPM Enterprise - Custom, Planning Modules • Legacy environments
EPM Standard - Consolidation and Close	• EPM Standard - Consolidation and Close • EPM Enterprise - Consolidation and Close	Legacy environments
EPM Enterprise - Consolidation and Close	• EPM Enterprise - Consolidation and Close • Legacy environments using Extended Dimensionality	• EPM Standard - Consolidation and Close • Legacy environments using Non-extended Dimensionality
EPM Enterprise - Tax Reporting	EPM Enterprise - Tax Reporting	• EPM Standard • Legacy environments
EPM Standard - Account Reconciliation	• EPM Standard - Account Reconciliation • EPM Enterprise - Account Reconciliation	Legacy environments

Table 4-2 (Cont.) Migration scenarios for EPM Standard and EPM Enterprise snapshots

Snapshot Source	Available Migration Paths	Unavailable Migration Paths
EPM Enterprise - Account Reconciliation	EPM Enterprise - Account Reconciliation	• EPM Standard - Account Reconciliation • Legacy environments
EPM Enterprise - Profitability and Cost Management	• EPM Enterprise - Profitability and Cost Management • EPM Enterprise - Enterprise Profitability and Cost Management	• EPM Standard • Legacy environments
EPM Standard - Narrative Reporting	• EPM Standard - Narrative Reporting • EPM Enterprise - Narrative Reporting	Legacy environments
EPM Enterprise - Narrative Reporting	EPM Enterprise - Narrative Reporting	• EPM Standard • Legacy environments
EPM Enterprise - Enterprise Data Management	• Oracle Fusion Cloud Enterprise Data Management • EPM Enterprise - Enterprise Data Management	• EPM Standard • Legacy environments

What Business Processes Can I Migrate to Cloud EPM?

The following business processes provide an option to migrate a snapshot in EPM Standard and EPM Enterprise environment:

- Account Reconciliation
- Enterprise Data Management
- Enterprise Profitability and Cost Management
- Financial Consolidation and Close
- Planning
- Profitability and Cost Management
- Tax Reporting

> **Note**
>
> Profitability and Cost Management, Enterprise Profitability and Cost Management, and Tax Reporting business processes are not available with EPM Standard.

These Migration Scenarios are Always Supported

- You can migrate an EPM Standard or EPM Enterprise business process. For example, after creating a snapshot of an EPM Standard business process, you recreated the service. You can use the snapshot to recreate the EPM Standard application.

- You can migrate a snapshot created in an EPM Standard or EPM Enterprise test environment to a production environment, and conversely.
- You can migrate snapshots from a legacy environment to another legacy environment.

These Migration Scenarios are Never Supported

- Migrating a snapshot from EPM Standard or EPM Enterprise to a legacy environment.
- Migrating a snapshot from EPM Standard, EPM Enterprise or legacy environments to on-premises deployments.

Migrating Account Reconciliation Snapshots

These migration Account Reconciliation scenarios are supported.

Source	Target
EPM Standard Cloud Application	EPM Enterprise Cloud Application
Legacy Account Reconciliation Cloud Application	EPM Enterprise Cloud Application
On-Premises Application (11.1.2.3 or 11.1.2.4)	EPM Standard Cloud or EPM Enterprise Cloud Application

Note

- Legacy application refers to an application from the latest update of a non EPM Standard or EPM Enterprise subscription.
- For instructions on migrating on-premises applications to Oracle Fusion Cloud Enterprise Performance Management, see "Migrating On-Premises Applications to EPM Cloud" in *Administering Migration*.

Migrating Enterprise Data Management Snapshots

You can migrate a snapshot from an EPM Enterprise - Enterprise Data Management business process to another similar environment or to a standalone Oracle Fusion Cloud Enterprise Data Management environment. If you are migrating snapshots from a Hosted Named User Metric subscription (Enterprise Data Management business process) that supports a maximum of 5,000 records, you can migrate to a Hosted Employee Metric subscription (Cloud EDM) that supports unlimited number of records. For information on the types of available options, see About Cloud EDM.

Some EPM Enterprise - Enterprise Data Management business process subscriptions have limits on the number of records in the environment. To determine if you comply with such limitations, before migrating snapshots, check the number of records in the environment using these steps:

1. Sign into your Enterprise Data Management.
2. In the **Settings and Actions** menu, click **About**, and then **Subscription**.

Migrating to Enterprise Profitability and Cost Management

Migration of on-premises Management Ledger applications to Enterprise Profitability and Cost Management involves these steps:

- Step 1: Packaging the Management Ledger application in a form that can be imported as a Profitability and Cost Management using the **Export Template** command of on-premises Oracle Hyperion Profitability and Cost Management. For instructions, see Using the Export Template Command in *Administering Migration*.
- Step 2: Uploading the package from the preceding step to Profitability and Cost Management using the Cloud Migration template to create a Profitability and Cost Management application.
- Step 2: Migrating the application from Profitability and Cost Management to Enterprise Profitability and Cost Management using the PCM to Enterprise Profitability and Cost Management Migration utility.

Your Goal	Watch This
Watch a video tutorial on migrating from Profitability and Cost Management to Enterprise Profitability and Cost Management	Tutorial

Migrating Financial Consolidation and Close Snapshots

These Financial Consolidation and Close migration scenarios are supported.

Source	Target
EPM Standard Cloud Consolidation and Close Application	EPM Standard Cloud Application
Legacy Consolidation and Close Application with Extended Dimensionality	EPM Enterprise Cloud Application
Legacy Consolidation and Close Application without Extended Dimensionality	EPM Enterprise Cloud Application* (* Not a standard migration; requires multiple steps to migrate)
On-Premises Application (11.1.2.3 or 11.1.2.4)	EPM Standard Cloud or EPM Enterprise Cloud Application

Note

- Legacy application refers to an application from the latest update of a non EPM Standard or EPM Enterprise subscription.
- For instructions on migrating on-premises applications to Oracle Fusion Cloud Enterprise Performance Management, see "Migrating On-Premises Applications to EPM Cloud" in *Administering Migration*.

To migrate a legacy application without Extended Dimensionality to an EPM Enterprise application, follow this process:

1. Create a backup snapshot by exporting the application from the source legacy environment. Download the backup snapshot to a local computer.
2. Enable Hybrid mode in the application by selecting **Application**, then **Overview**, then **Actions** and then **Enable Hybrid Mode**. For detailed information, see "Migrating to Extended Dimensionality" in *Administering Financial Consolidation and Close*.
3. Export the application from the source legacy environment and import it into the destination EPM Enterprise.

Migrating Planning Snapshots

These Planning migration scenarios are supported.

Source	Target
EPM Standard Cloud Planning Application	Modules-based EPM Enterprise Cloud Application
Legacy Planning and Budgeting Cloud Application	Custom Application in EPM Enterprise Cloud
Enterprise Planning and Budgeting Cloud or Planning and Budgeting Cloud with Plus One Option Application	Modules-based application in EPM Enterprise Cloud
On-Premises Planning Application (11.1.2.3, 11.1.2.4, or 11.2.x*)	EPM Standard Cloud or EPM Enterprise Cloud Application

* 11.2.x On-Premises Planning applications that use Essbase 21c cannot be migrated to EPM Cloud

Note

- A legacy application refers to an application from the latest update of a non-EPM Standard or EPM Enterprise subscription.
- Migration of applications from legacy Planning and Budgeting Cloud, Enterprise Planning and Budgeting Cloud, and Planning and Budgeting Cloud with Plus One option creates standard BSO cubes, which you may convert to Hybrid cubes.
- For instructions on migrating on-premises Planning applications to Oracle Fusion Cloud Enterprise Performance Management, see Migrating On-Premises Applications to EPM Cloud in *Administering Migration*.

Note

Attempts to import Groovy-based business rules and templates into a business process that does not support Groovy will fail. For example, EPM Standard Financial Consolidation and Close business processes do not support Groovy-based business rules. Import of business rules and templates exported from an application that supports Groovy, for example, from an EPM Enterprise Financial Consolidation and Close business process, into EPM Standard Financial Consolidation and Close business process, will fail.

Migrating Profitability and Cost Management Snapshots

These Profitability and Cost Management migration scenarios are supported.

Source	Target
Legacy Profitability and Cost Management Cloud Application	Profitability and Cost Management
On-premises Standard or Management Ledger Application (11.1.2.4)	

> **Note**
>
> - Legacy application refers to an application from the latest update of a non EPM Standard or EPM Enterprise subscription.
> - For instructions on migrating on-premises Profitability and Cost Management snapshots to EPM Enterprise. See "Migrate Profitability and Cost Management to Oracle Profitability and Cost Management Cloud" in *Administering Migration*.

Migrating Tax Reporting Snapshots

You can migrate a snapshot from the newest update of a legacy Tax Reporting application to EPM Enterprise to create a business process.

Migrating to Cloud EDM

Enterprises that currently have Hosted Employee Metric or Hosted Named User Metric subscription of the Enterprise Data Management business process can migrate to the standalone Oracle Fusion Cloud Enterprise Data Management. See About Cloud EDM.

You can migrate from On-Premises 11.1.2.4.330 or newer Oracle Data Relationship Management to the standalone Cloud EDM to exercise the full power of this solution as a change management and governance solution for master data, reference data or metadata anywhere in the public, private or hybrid cloud be it from Oracle, a third-party, or a bespoke application.

For information on migrating from Data Relationship Management, see About Data Relationship Management Migration.

About Essbase in Cloud EPM

> **Note**
>
> Enterprise Data Management does not use Oracle Essbase.

In this section:

- Data Values in Essbase

- Essbase in EPM Standard and EPM Enterprise Subscriptions
- Enabling Hybrid Mode for Your Application
- After Enabling the Use of Hybrid BSO Cubes, Can I Revert to Using Non-hybrid Cubes?
- How Do I Know if an Application has Hybrid BSO Cubes Enabled?

Data Values in Essbase

Essbase uses IEEE double values to represent cell values, which offer a maximum precision of 15 significant digits. However, beyond the 15th digit, it becomes imprecise. It's important to distinguish between significant digits and digits after the decimal point; for instance, the number 497.1 has four significant digits. When stored as a double, its accuracy extends up to the 12th digit after the decimal, constituting the 15th significant digit.

Certain decimal values can't be perfectly represented in binary, resulting in slight variations when loaded into Essbase and queried. For instance, loading -132.35 might display as -132.3499999... until rounded to 12 decimals, yielding the expected result of -132.3500000...

Furthermore, a number like -132.349999999999 remains accurate to at least 15 significant digits. Occurrences of "9" in the sixth significant digit don't imply accuracy limited to six significant digits; they indicate a deviation of minus one in the 15th significant digit. If the deviation were plus one, the result would be -132.350000000001.

It's crucial to note that differences in hardware and compilers introduce slight variances in results across different platforms. For more information see The Limits of Data Precision in Essbase.

Essbase in EPM Standard and EPM Enterprise Subscriptions

EPM Standard and EPM Enterprise subscriptions are deployed with an Essbase version that supports Hybrid Block Storage Option (BSO) cubes. Hybrid cubes may be used by Financial Consolidation and Close, Planning Application types such as Custom Planning, Strategic Workforce Planning and Sales Planning. If you create a FreeForm application by importing a snapshot from an Essbase deployment that does not support Hybrid cubes, the FreeForm application will then use non-hybrid BSO cube. See Available Cloud EPM Subscriptions.

To make parent members of sparse and dense dimension dynamic, the Hybrid BSO cubes support some Aggregate Storage Option (ASO) capabilities in addition to BSO capabilities. For example, all cubes can have dynamic aggregations for calculations. Hybrid cubes provide many benefits including smaller database and application size, better cube refresh performance, faster import and export of data, improved performance of business rules, and faster daily maintenance of the business process. To ensure optimal performance, warnings and error messages are displayed during cube refresh if the business process does not conform to best practices for the following parameters:

- Block size
- Number of blocks
- Number of dense dimensions
- Maximum number of child members under any dynamic parent
- Maximum number of child members under any store parent
- Parents with one child member for level 1 and above of dimensions
- Level 1 and above not set to dynamic calculation and label only in dense dimensions
- Usage of dynamic cross-references

These parameters of enabled modules are enforced to ensure that best practices are followed:

- Number of new rules that can be added to a module
- Number of rules that can be modified
- Number of new forms added to a module
- Number of forms that can be modified

Enabling Hybrid Mode for Your Application

If you have a legacy Oracle Enterprise Planning and Budgeting Cloud subscription or a Planning and Budgeting Cloud Service Plus One option license, you can convert your Planning application to use Hybrid BSO cubes.

1. Convert the Planning application in your test environment to a Planning Modules application.
   See "Converting a Standard or Reporting Application to an Enterprise Application" in *Administering Planning Modules.*
2. Refresh the database. Ensure that the process runs successfully without errors. See Creating and Refreshing Application Databases in *Administering Planning*.
3. Enable Hybrid.
   a. From the Home page, select **Application** and then **Overview**.
   b. From **Actions**, select **Enable Hybrid Mode**.
      Oracle Fusion Cloud Enterprise Performance Management validates your application to ensure that it meets the requirements for applications that use Hybrid cubes. These best practices are listed at the beginning of this section.
   c. Modify your application based on the validation errors and warnings. Errors must be resolved before a successful database refresh can occur. On encountering an error, the database refresh process stops and places the application into maintenance mode. Warnings must be reviewed to identify and correct potential issues.
   d. **Optional:** Redesign and streamline your application to make best use of Hybrid BSO capabilities. Steps to streamline your application include making parent members in some sparse dimensions dynamic and removing intermediate rollups from rules, where appropriate. Additionally, you may need to modify the existing member formula syntax. Test the application to determine the right combination of sparse dimensions with dynamic parent members that work for your specific application.
4. Test your application to verify that it works as designed.
5. Repeat the preceding steps to convert the application in the Production environment.

After Enabling the Use of Hybrid BSO Cubes, Can I Revert to Using Non-hybrid Cubes?

The availability of the option to disable the hybrid mode depends on whether your environment supports it. Additionally, only these business processes or application types allow you to disable the hybrid mode:

- Planning Custom applications
- FreeForm

> **⚠ Caution**
>
> Before disabling the hybrid mode, carefully review the sparse dimension configuration to ensure that the upper level members set to *Dynamic Calc* with hybrid mode enabled are reverted to *Store* or *Never Share*, as appropriate, in non-hybrid mode. Additionally, review rules to include the sparse dimensions that were set to *Dynamic Calc* for parent members for aggregations and other rules, as appropriate.

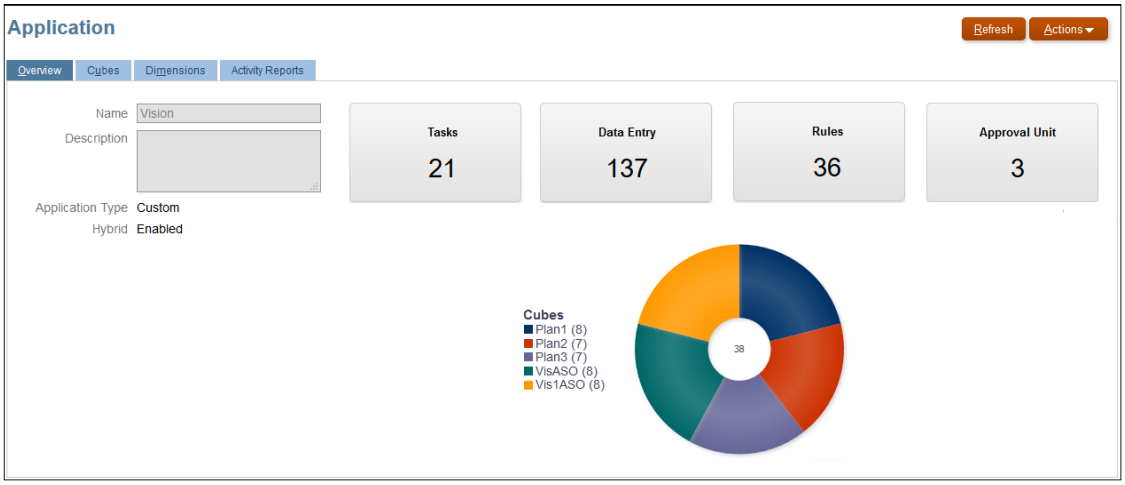
To disable the use of hybrid BSO cubes:

1. Sign into the application as a Service Administrator.
2. Select **Application** and then **Overview**.
3. Click **Actions** and then select **Disable Hybrid Mode**.

How Do I Know if an Application has Hybrid BSO Cubes Enabled?

The Overview tab of your application indicates whether it is set up to use Hybrid cubes. You can open this tab from the Home page by selecting **Application** and then **Overview**.

As a general guideline, Financial Consolidation and Close, Custom Planning, Planning Modules, and FreeForm applications that you create in EPM Enterprise use Hybrid BSO cubes. Additionally, Financial Consolidation and Close and Planning Modules applications you create in EPM Standard environments, by default, use Hybrid BSO cubes. Some cubes in these applications may still use ASO cubes, as necessary or as delivered content by Oracle.



5

Configuring Cloud EPM and Cloud EDM Environments

In This Section:

Sample URLs

You use a unique URL to access Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. A Service Administrator provides these URLs to users.

> **Note**
>
> You cannot modify the URLs. If the URLs seem difficult to remember, use vanity URLs or create unique bookmarks to make it easier to enter them into your browser. For more information, see Using Vanity URLs in *Getting Started Guide for Administrators* .

OCI Cloud EPM and Cloud EDM environments use the following URL pattern:

`https://ENVIRONMENT_NAME-CLOUD_ACCOUNT_NAME.epm.REGION.ocs.oraclecloud.com/epmcloud`

> **Note**
>
> This pattern is for commercial regions only. In restricted regions (for example OC2 and OC4) , the patterns are different. Environments that are migrated to OCI using Oracle-Managed Migration keep their Classic URL pattern. For example: `https://epm-idDomain.epm.dataCenter.oraclecloud.com/epmcloud`.

Table 5-1 URL Components

Name	Description
Environment Name	The environment name, for example, `acme` or `acme-test`, specified while creating the environment.
Cloud Account Name	This is the name, for example, `epmidm` used while creating the Oracle Fusion Cloud EPM Account.
Region	This is the region where the data center that hosts the environment is located. This is selected when you create the environment, for example, `us-phoenix-1`.

> **Note**
>
> See Creating an Environment in *Getting Started Guide for Administrators* for information on these values.

Using the sample settings from the preceding explanation, the URLs may be as follows:

Production environment: `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/epmcloud`

Test environment: `https://acme-test-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/epmcloud`

Setting Up Browsers

In This Section:

Supported Browsers

Lists the supported and recommended browsers for each client platform.

To comply with Oracle Support policies, you must use a supported browser while accessing the Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment. See Oracle Software Web Browser Support Policy.

Table 5-2 Supported Browsers for Each Client Platform

Client Platforms	Recommended Browser	Other Supported Browsers
Microsoft Windows	Google Chrome	Firefox ESR Microsoft Edge Version 80 or newer
Apple Mac OS X	Google Chrome	Safari, Firefox ESR
Linux (all versions)	Google Chrome	Firefox ESR
iOS *	Safari	None
Android *	Google Chrome	None

Table 5-2 (Cont.) Supported Browsers for Each Client Platform

Client Platforms	Recommended Browser	Other Supported Browsers
* Only browser-based interaction is supported for iPads and Android mobile devices. Browser-based interaction is not supported on phones.		

To ensure access to the service, you must configure your browser to:

- Accept cookies from `oraclecloud.com` and `cloud.oracle.com` By default, the browsers are set up to accept cookies from websites. If your browser is configured to not accept cookies from sites, you must allow a per session or permanent exception for these sites
- Allow pop-up windows from `oraclecloud.com` and `cloud.oracle.com`

Using Multiple Browser Tabs or Browser Instances

The business processes require each user to maintain a separate browser session. Additionally, the Cloud EPM or Cloud EDM environment support only one instance of dashboards per browser session.

Business processes may not refresh correctly if you have multiple sessions open at the same time on the same machine. For example, this can occur if you have one Chrome window with two tabs or multiple instances of the same browser(say two Chrome windows). Running multiple simultaneous operations using the same user ID from either the same computer or different computers may also result to unpredictable behavior.

A **Duplicate Tab** command is available in Firefox, Chrome, and Edge browsers to spawn another instance of the current tab. However, Oracle does not recommend using this command to duplicate the current view of a business process, as it may result in the display of errors within the business process.

Configuring Google Chrome for a Translated Version of the Service

You update the language settings of Google Chrome to access the service in a language other than the default browser language. For a list of languages in which the service is available, see Understanding Translation.

To reconfigure Chrome for a new locale:

1. In Google Chrome, access Settings by navigating to `chrome://settings/`
2. Click **Settings**, then **Advanced**, and then **Languages**.
3. From **Language** drop-down list, select **Add Languages**.
4. In **Add Languages**, select the display language for the service and then click **ADD**.
5. Click **More actions** next to the display language for the service that you added in the preceding step and then select **Display Google Chrome in this Language**.
6. Click **RELAUNCH** .

   Google Chrome restarts in the selected language.

Configuring Microsoft Edge

You can update the language settings in Microsoft Edge to access Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments in a language other than the default language set in the browser.

General Settings

Make sure that Microsoft Edge is configured to allow JavaScripts, cookies, and pop-ups. These are allowed by default.

- If your organization does not allow the default setting, make sure to add `*.oraclecloud.com` as an allowed site. You can view the current JavaScript setting by accessing the URL `edge://settings/content/javascript`
- If pop-ups are blocked, make sure to add `*.oraclecloud.com` as an allowed site. You can view the current pop-up setting by accessing the URL `edge://settings/content/popups`
- If the use of cookies is blocked, add `*.oraclecloud.com` as a site from which cookies should be accepted. You can view the current cookie setting by accessing the URL `edge://settings/content/cookies`

Configuring Microsoft Edge for a Translated Version of the Service

For a list of languages in which the service is available, see Understanding Translation.

To configure Microsoft Edge for a new locale:

1. Open your Microsoft Edge browser and enter the URL `edge://settings/languages`
2. If the locale you want to use is not listed under **Preferred languages**, click **Add languages** and add it.
3. Under **Preferred languages**, click ... (**More actions)** in the row of the locale you want Microsoft Edge to use, and then select **Display Microsoft Edge in this language**.
4. Click **Restart**.

Configuring Firefox

Configuring Firefox involves enabling the pop-ups and modifying privacy settings.

Firefox, by default, is configured to accept cookies from websites. If your browser is configured to not accept cookies from sites, you must allow a per-session or permanent exception for `cloud.oracle.com` and `oraclecloud.com`. You must also allow Firefox to open pop-up windows from these websites.

To configure Firefox to accept cookies and enable pop-ups:

1. Start Firefox
2. Select **Tools**, then **Options**, and then **Privacy**.
3. Verify the setting in the **Firefox will** field:
   - If the value is set to **Remember history** or **Never remember history**, your browser will use default settings to correctly display the service.
   - If the value is set to **Use custom settings for history**:
     - Verify that the **Accept cookies from sites** check box is selected (checked).

- Click **Exceptions**, and remove any exception that prevents the following websites from setting cookies:
  - `cloud.oracle.com`
  - `oraclecloud.com`

  If the **Accept cookies from sites** check box is not selected, complete the following steps:

a. Click **Exceptions**.

b. In **Address of web site**, enter `cloud.oracle.com`, and then click either **Allow** or **Allow for session**, depending on your privacy policies.

c. Repeat step 3.b to add `oraclecloud.com`.

d. Click **Save Changes**.

4. Enable pop-up windows from `cloud.oracle.com` and `oraclecloud.com`, and, optionally, enable pages to choose their own fonts.

a. Click **Content**.

b. If **Block pop-up windows** is selected (checked), click **Exceptions**.

c. In **Address of web site**, enter `oraclecloud.com`, and then click **Allow**.

d. In **Address of web site**, enter `cloud.oracle.com`, and then click **Allow**.

e. Click **Save Changes**.

f. **For Narrative Reporting only:** enable pages to choose their own fonts.

i. Click **Advanced** under **Fonts & Colors**.

ii. Select **Allow pages to choose their own fonts, instead of my selections above**.

iii. Click **OK**.

Configuring Firefox for a Translated Version of the Service

You update the language settings of Firefox to access the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environment in a language other than the default browser language.

For a list of languages in which the service is available, see Understanding Translation.

> **Note**
>
> Narrative Reporting can override the browser locale by setting a preferred locale. See Managing User Preferences in *Administering Narrative Reporting* for details.

To modify language settings:

1. In Firefox, select **Tools**, and then **Options**.
2. Click **Content** to open the Content page.
3. Click **Choose** next to **Languages**.
4. **Optional:** If the language that you want to use is not listed in **Languages**, add it using these steps:

a. In **Languages**, click **Select a language to add...**.

b. Select the desired language, and then click **Add**.

5. Click the desired language and then click **Move Up** to move it to the top of the list.

6. Click **OK**.

Recommended Screen Resolution

Oracle recommends that you set the screen resolution of your display unit to 1920 x 1080. Additionally, the maximum window scale setting should be set to 125%.

Accessing Cloud EPM and Cloud EDM Environments

You can access Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments using the user or Single Sign-On (SSO) credentials.

For instructions to authenticate, see:

- Authenticating Using User Credentials
- Authenticating Using Single Sign-On Credentials

SSO access between the Cloud EPM and Cloud EDM environment and deployments of Oracle Fusion, and NetSuite is also available. Additionally, SSO can be provided by integrating your services with Identity Cloud Service. See Managing Single Sign-On in *Administering Oracle Cloud Identity Management* for information on configuring the SSO process to work with the identity provider that your organization uses. Additionally, your IT administrator may configure browsers for Integrated Windows Authentication (IWA) to allow you to access the service without entering your credentials.

> **Note**
>
> Clients such as EPM Automate do not work with SSO credentials. The user accounts for accessing such clients must be maintained in the environment.

Troubleshooting

For common issues related to the environment, see in *Operations Guide*:

- Resolving Login Issues
- Dealing with Down Environments
- Dealing with FastConnect Issues
- Resolving IP Allowlist Functional Issues
- Managing Patching Issues
- Managing Other Functional Issues
- Resolving Other Performance Issues

Authenticating Using User Credentials

The first time you log in, check the email from Oracle Fusion Cloud EPM Administrator (`oraclecloudadmin_ww@oracle.com`) for your user name and a temporary password. Check the email from your Service Administrator for the URL to access the service.

You must have the following information:

- URL to access the environment
- A username
- A password

To access the environment:

1. Go to the provided URL.
2. Enter your **User Name** and **Password**.
3. Click **Sign In**.
   - If you have already reset your default password, the Home page is displayed.
   - If this is your first time accessing the service, you'll be directed to the **Password Management** screen to set your password.
4. To set your password:
   a. In **Old Password**, enter the temporary password that you received in the email from Cloud EPM Administrator (`oraclecloudadmin_ww@oracle.com`).
   b. In **New Password** and **Re-Type Password**, enter a new password that conforms to the password policy displayed on screen.
   c. In **Register challenge questions for your account**, select challenge questions and their answers. These are used to retrieve the password if you forget it.
   d. Click **Submit**.

Authenticating Using Single Sign-On Credentials

The sign-in process is governed by your organization's SSO configuration. If your setup uses IWA, you may not be prompted to enter a username and password when you access the Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment.

To access an environment using your SSO credentials:

1. Go to the provided URL of the environment.
2. Click **Company Sign In**.

> **Note**
>
> In SSO enabled environments, **Company Sign In** is the only option available to most users. Service Administrators and Account Reconciliation Power Users, whose accounts are configured to run the client components such as EPM Automate, will see an additional option to sign in using Traditional Cloud Account.

If you are in a setup that uses IWA, the landing page of the service is displayed. Otherwise, a login screen is displayed.

3. If a sign in screen is displayed, enter the user name and password that you use to access your organization's network resources, and then click **OK**.

Changing Your Password

On your first login, you'll be asked to personalize your password and set challenge question answers for password recovery.

Oracle Fusion Cloud Enterprise Performance Management environments can be configured to set password policy to match your corporate standard. In *Administering Oracle Identity Cloud Service*. See:

- Manage Oracle Identity Cloud Service Password Policies
- Changing Your Password

In environments configured for Single Sign-on with an identity provider, the password policy for signing into an environment using the **Company Sign In** option is managed by the identity provider.

To change your password:

1. In a browser, enter the URL of the environment for which you want to change your password.

   Changing password affects your password all the environments in that IAM domain.
2. Click **Forgot Password**.
3. In the **What's your user name?** field, enter your user ID, for example, `john.doe@example.com`.

   A password reset notification will be sent to the recovery email address associated with your username.
4. Open the recovery email and click **Reset Password**.
5. In the **Enter new password** and the **Re-enter new password** field, enter the a new password.
6. Click **Reset Password**.

   You will see a confirmation message. A confirmation email is also sent to your email address.

Exploring the User Experience

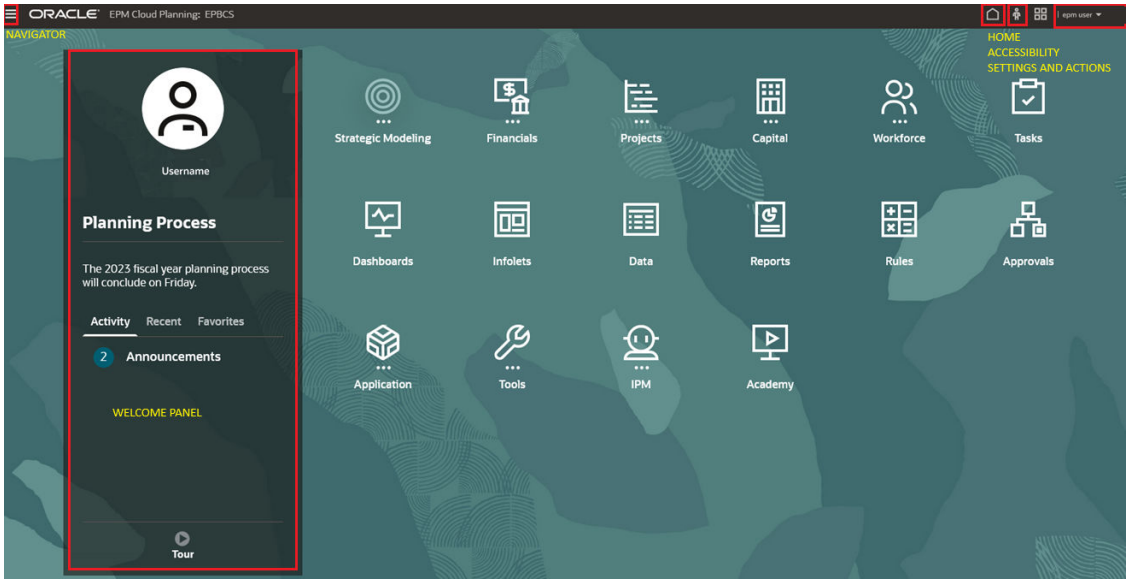
Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments utilize the Redwood Experience, which offers a modern interface with unique features.

The Home Page

When you sign in to an environment, you will be taken to the Home Page.

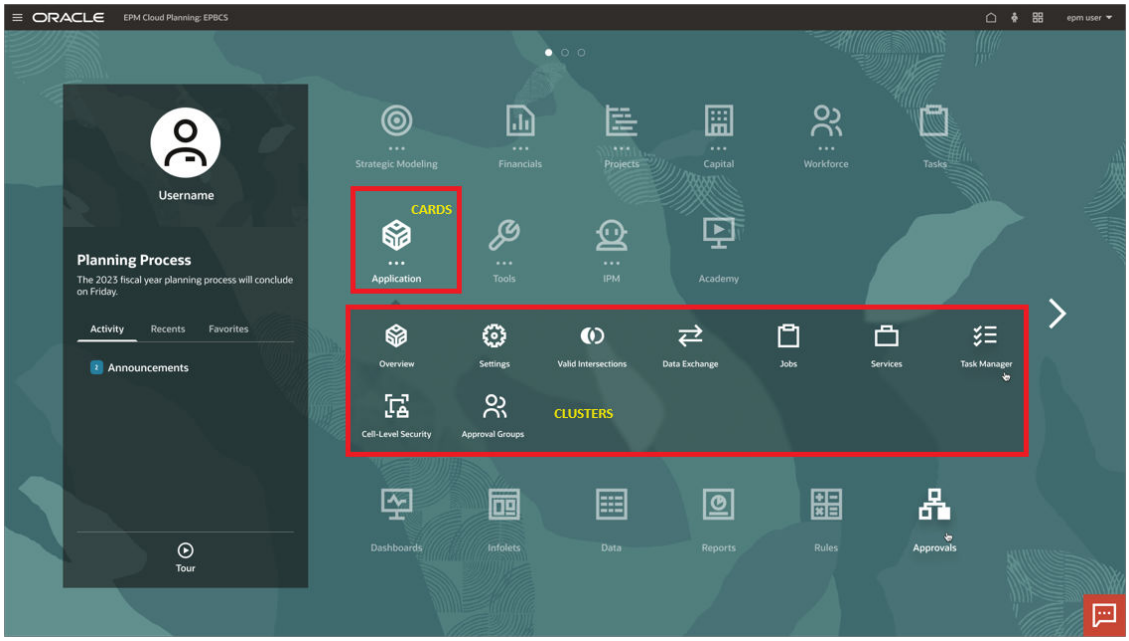
- **Navigator** - In the top-left corner, you'll see the Navigator icon. Click it to open a list of shortcuts that match the features and functions available on the Home Page cards.

- **Welcome Panel** - This is located in the center-left of the screen and gives you quick access to important info, like your messages and tasks. The details here may change depending on the service you're using.
- **Home** - On the top-right corner, this icon lets you return to the Home Page from anywhere in the environment.
- **Accessibility** - Right next to the Home icon, the Accessibility icon helps you adjust settings like screen readers and high contrast mode.
- **Settings and Actions**- Click your user name in the top-right corner to access settings such as Help, Provide Feedback, Oracle Support, Sign Out and more. Additionally, you can join Oracle Cloud Customer Connect, a community where members collaborate on common goals and objectives. See Joining Oracle Cloud Customer Connect.



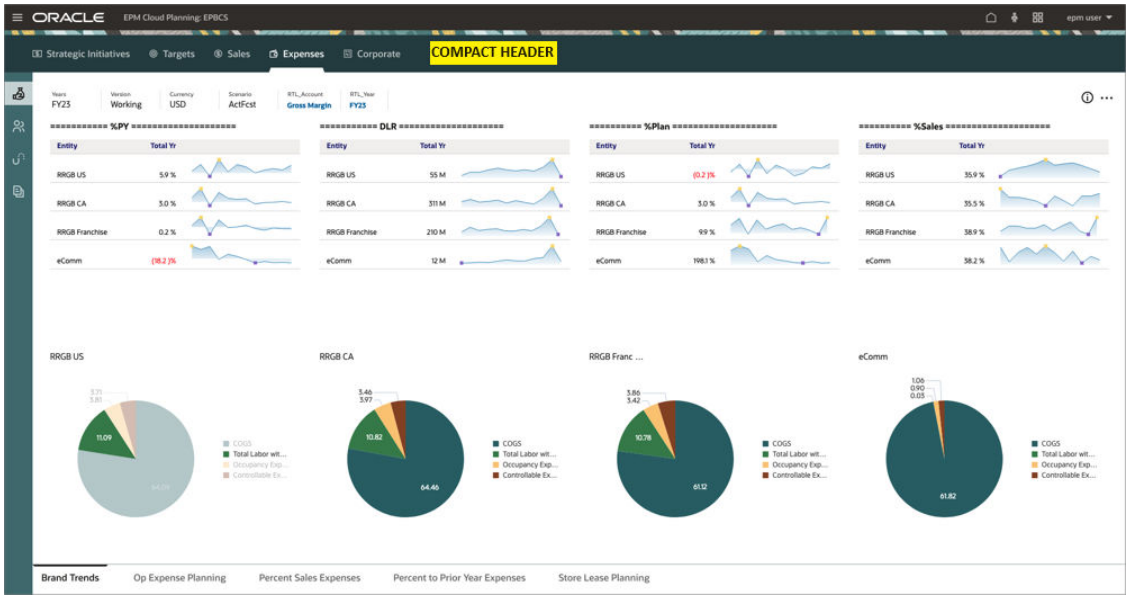
Simplified Cards and Clusters Identification

The Home Page features cards that group various activities you can perform in the environment. These cards offer access to key tasks, tutorials, and related information. Clicking on a card opens a page with available shortcuts, which vary based on your role in the environment. Each card is highlighted with its related cluster of features expanded underneath, making it easier to identify. This layout maintains the existing navigation flow while simplifying the process of locating cards.



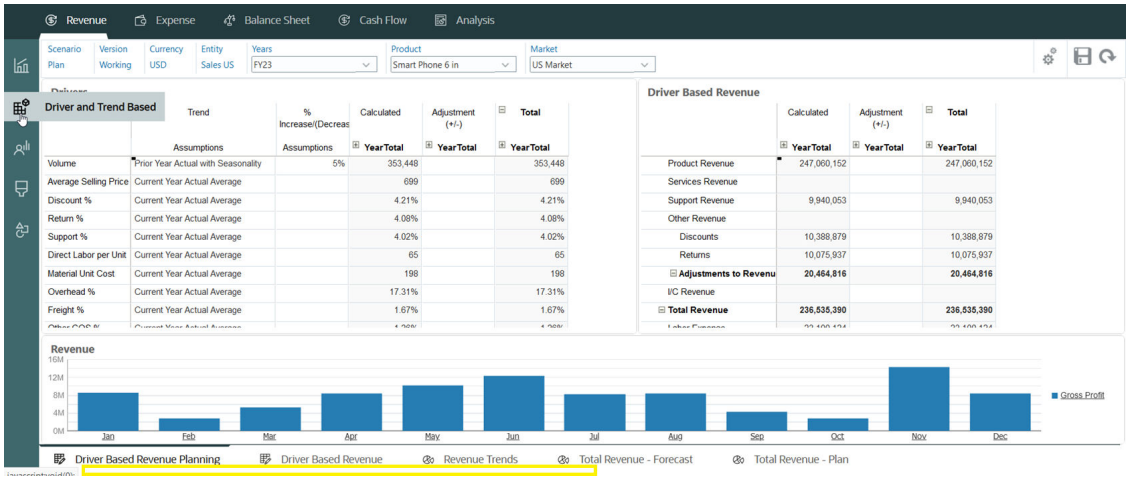
Compact Headers

When you open a card to view a service capability, compact headers at the top of the screen help save space. These headers make it unnecessary to expand or collapse the screen to see information. The color of the compact header matches the selected theme and saves approximately 90 pixels of vertical space, creating more room for URL display at the bottom.



Tabs Positioning

The tabs are located in the left pane, with their corresponding sub-tabs positioned at the bottom of the page for improved clarity and navigation. When you hover over a vertical tab, the tab name appears directly rather than a tooltip. Additionally, more space is allocated to the bottom tab to better accommodate URL display.



Overview of Creating a Business Process

The Oracle Fusion Cloud Enterprise Performance Management landing page serves as your starting point for creating a Cloud EPM business process and viewing overview videos.

Before you get started:

1. Create a production and a test Cloud EPM environment with your subscription. See Creating an Environment.
2. Sign in to the environment as a Service Administrator. See Accessing Cloud EPM and Cloud EDM Environments.

New customers will see one of the following landing pages based on the type of subscription purchased:

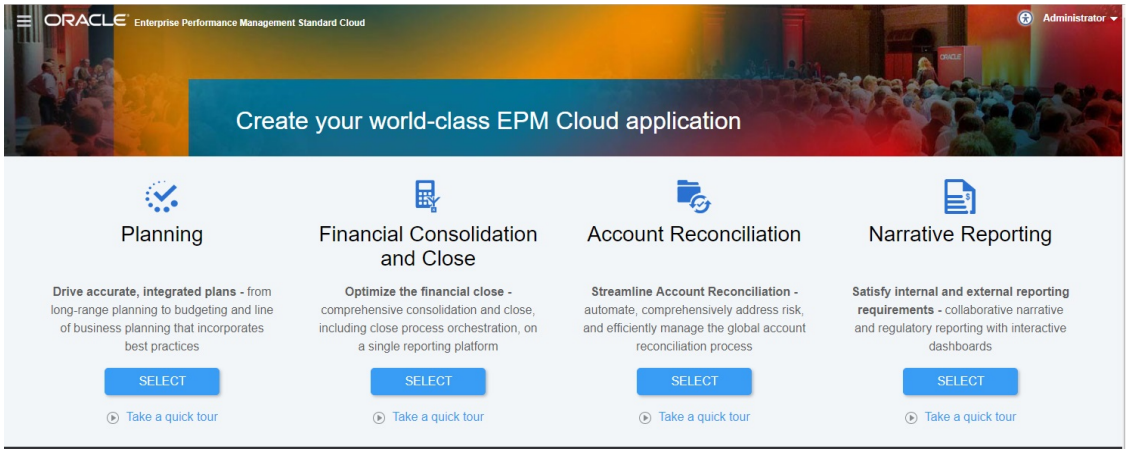
- EPM Standard landing page
- EPM Enterprise landing page

Selecting a business process will initiate the setup process.

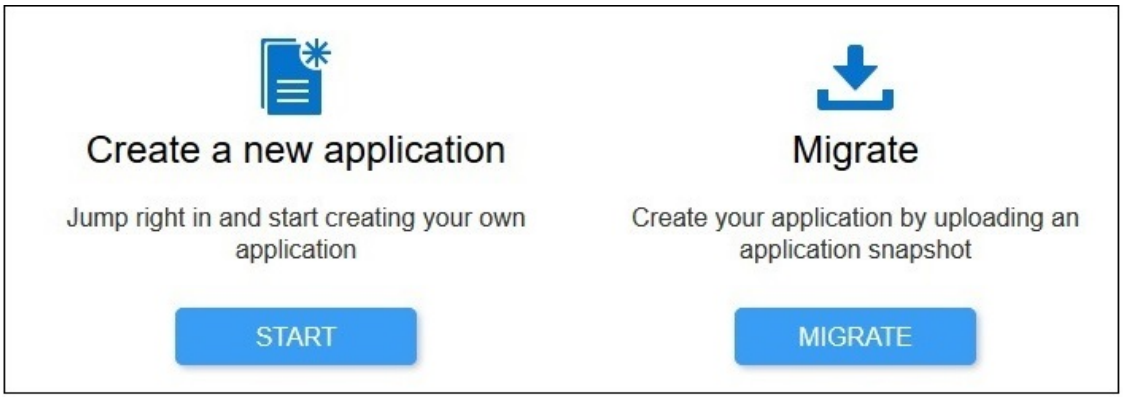
Creating a Business Process from EPM Standard Landing Page

Each EPM Standard subscription allows you to create one business process.

The landing page is your starting point for creating a business process. To get an overview of the business processes available in the standard subscription, see Available Cloud EPM Subscriptions .



Click **SELECT** under the business process description to see available options.



- Click **START** to create a new business process for the specific business application
- Click **MIGRATE** to import a business process from a snapshot that you previously uploaded to the environment. See What Business Processes Can I Migrate to Cloud EPM? for prerequisites and snapshot compatibility.

You can create the following business processes from the EPM Standard landing page. For detailed procedures, see these information sources:

- **Account Reconciliation**: See Pre-configuring Your Environment in *Administering Oracle Account Reconciliation*
- **Financial Consolidation and Close**: See Creating an EPM Standard Cloud Service Application in *Administering Financial Consolidation and Close*
- **Narrative Reporting**: See EPM Standard Cloud Service Landing Page in *Administering Narrative Reporting*
- **Planning**: See Creating an EPM Standard Cloud Service Application in *Administering Planning*

Once you create an application, the application home page is displayed when you log in; the landing page is no longer displayed.

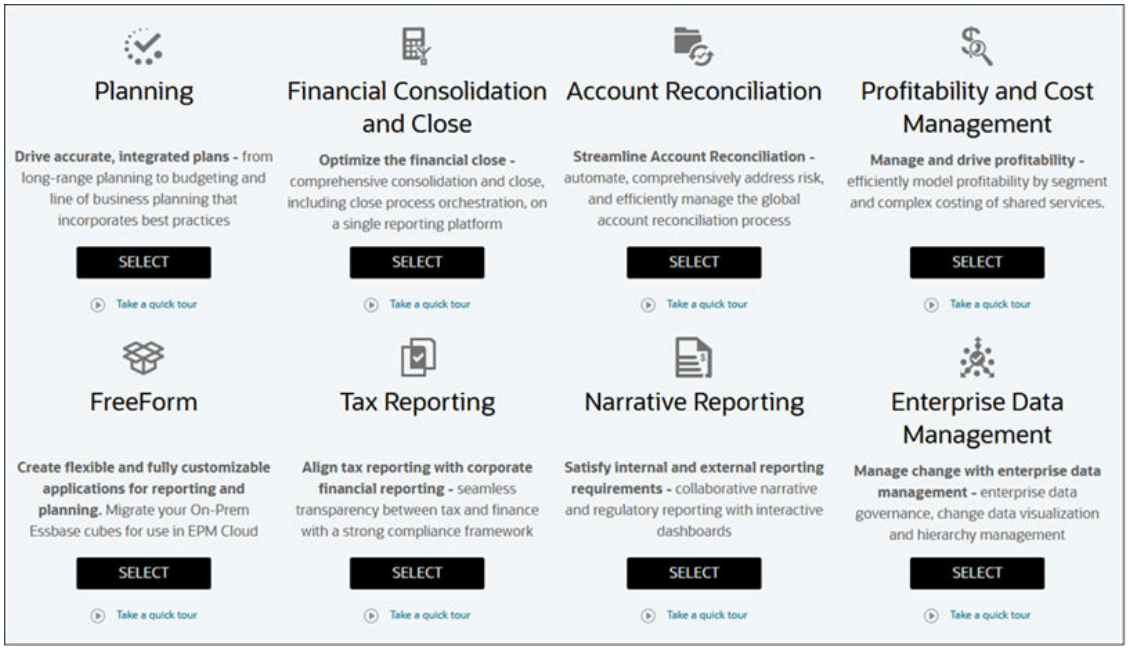
In case you decide to return to the landing page to switch to a different business process, you will have to first reset your environment to its original state. To do this, click your username on top-right, and then select **Recreate Service**.

For more information, see Switching to a Different Cloud EPM Business Process.

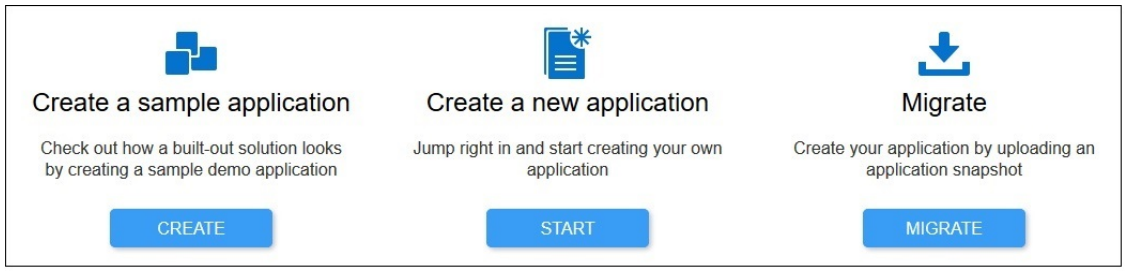
Creating a Business Process from EPM Enterprise Landing Page

Each EPM Enterprise allows you to create one business process.

The landing page is your starting point for creating a business process (application). To get an overview of the business processes available in the enterprise subscription, see Available Cloud EPM Subscriptions.



Click **SELECT** under the business process description to see these available options:



- Click **CREATE** to automatically create a sample application
  The Sample application contains artifacts and data and lets you quickly explore the business process. Not all business processes support the sample application. See the Administration Guide of your business process for more information:
- Click **START** to create a new business process
- Click **MIGRATE** to import a business process from a snapshot that you previously uploaded to the environment. See What Business Processes Can I Migrate to Cloud EPM? for prerequisites and snapshot compatibility.

> **Note**
>
> Some business processes do not give the option to create a sample application.

You can create the following business processes from the EPM Enterprise landing page. For detailed procedures, see these information sources:

- **Account Reconciliation**: See Pre-configuring Your Environment in *Administering Oracle Account Reconciliation*
- **Oracle Fusion Cloud Enterprise Data Management**: See Pre-Configuring Your Environment in *Administrating and Working with Enterprise Data Management Cloud*
- **Enterprise Profitability and Cost Management**: See Pre-configuring Your Environment in *Administering and Working with Enterprise Profitability and Cost Management*
- **Financial Consolidation and Close**: See Creating an EPM Enterprise Cloud Service Application in *Administering Financial Consolidation and Close*
- **FreeForm**: See Creating a FreeForm App in *Administering FreeForm*
- **Narrative Reporting**: See EPM Enterprise Cloud Service Landing Page in *Administering Narrative Reporting*
- **Planning**: See Creating an EPM Enterprise Cloud Service Application in *Administering Planning*
- **Profitability and Cost Management**: See Creating a Profitability and Cost Management Application in *Administering Profitability and Cost Management*
- **Tax Reporting**: See Creating an EPM Enterprise Cloud Service Application in *Administering Tax Reporting*

Once you create an application, the application home page is displayed when you log in; the landing page is no longer displayed.

In case you decide to return to the landing page to switch to a different business process, you will have to first reset your environment to its original state. To do this, click your username on top-right, and then select **Recreate Service**.

For more information, see Switching to a Different Cloud EPM Business Process.

Switching to a Different Cloud EPM Business Process

You can switch to another business process by recreating your Oracle Fusion Cloud Enterprise Performance Management environment. Recreating the environment deletes the current business process, including all user-defined (custom) artifacts and data from the environment and returns it to its original state. This process can also be used to remove all traces of the current business process and build a new one. Once the process starts, the environment is not available for approximately 20 minutes.

> **Note**
>
> If you want to preserve the data and artifacts in the current environment, perform a complete backup.

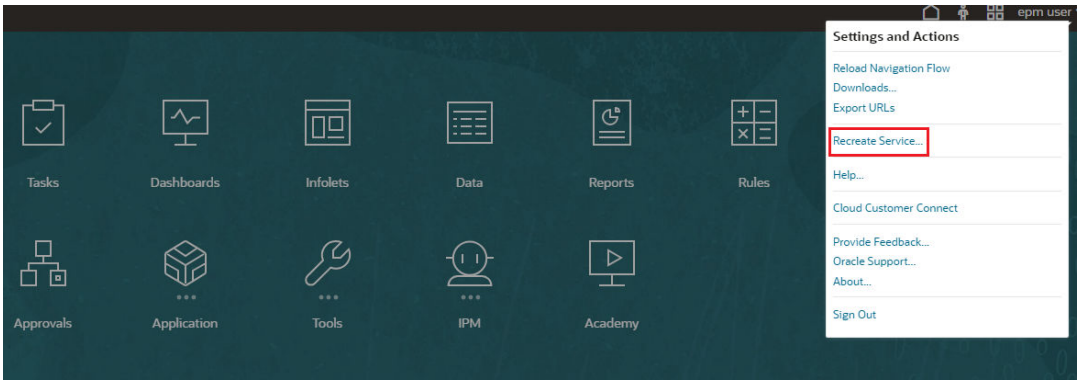
Recreation does not change any of the following:

- Snapshot created during the last maintenance of the environment. Cloud EPM always retains the maintenance snapshot
- Users that you created in the identity domain that use the environment
- Users to predefined role assignments

> **Note**
>
> You can also recreate an environment using EPM Automate or REST API. See:
>
> - Recreate Service in *Working with EPM Automate*.
> - Run Recreate on a Service in the *REST APIs for Oracle Fusion Cloud EPM* guide.

Recreating a Service (Business Process)

1. On the Home page, access **Settings and Actions** by clicking your user name at the top right corner of the screen.



2. Select **Recreate Service**.
3. Click **OK** to initiate the recreate process and to confirm that you are aware of the consequences of re-creating the Cloud EPM environment.

Transitioning from Enterprise Data Management Business Process to Cloud EDM

When transitioning from Enterprise Data Management business process to standalone Oracle Fusion Cloud Enterprise Data Management, consider the following key factors:

Email Notification

The email notification received upon provisioning labels the new environment as an Oracle Fusion Cloud Enterprise Performance Management environment, when it is actually the standalone Cloud EDM. It's important to clarify that no transition to Cloud EPM is needed, and the environment is indeed standalone Cloud EDM with the correct configuration and usage.

Setting Up Cloud EDM on the Same Domain

You can set up the standalone Cloud EDM on the same domain as the existing Enterprise Data Management business process, as long as both the cloud account and identity domain are part of the same primordial stripe.

Setting Up Cloud EDM on the Same URL

It is not possible to set up the Cloud EDM on the same URL unless you move the existing environment to a new location. The process involves:

- Resetting the environment.
- Creating a new Cloud EDM subscription using the original Enterprise Data Management business process name.
- Performing a clone operation.

For example, if your existing cloud account has the Enterprise Data Management business process name as `edm1/edm1-test`, follow these steps:

1. Move the app and data to a temporary holding location, such as `epme3/epm3-test`.
2. Clone the environment from `edm1/edm1-test` to `epme3/epm3-test`.
3. Delete the original environment, `edm1/edm1-test`.
4. Once the deletion is processed, create a new Cloud EDM environment within the Oracle cloud account and assign the service name `edm1`.
5. After the new Cloud EDM environment is created, clone the environment from `epme3/epm3-test` back to `edm1/edm1-test`.

This double clone process is only necessary if you wish to retain the same URL and business process name.

Using the Same Identity Domain and SSO for Cloud EDM

You can use the same identity domain and Single Sign-On (SSO) setup when transitioning from the Enterprise Data Management business process to Cloud EDM. However, you will need to assign the appropriate access and permissions within the Oracle Identity Cloud to ensure users have the necessary access rights.

Joining Oracle Cloud Customer Connect

Customer Connect is a community gathering place for members to interact and collaborate on common goals and objectives. It's where you will find the latest release information, discussion forums, upcoming events, and answers to use-case questions. Joining takes just a few minutes. Join now and sign up for notifications!

To Join Customer Connect:

1. Go to https://community.oracle.com/customerconnect/ and select **Register** in the upper right.
2. After you have joined and logged in, access the forums (categories), from the Cloud Customer Connect home page. Select **Categories**, then **Enterprise Resource Planning**, and then make your selection under **Enterprise Performance Management**.

To ensure you are always in the know, confirm you have your notification preferences set for EPM Announcements as well as each category you're following.

1. To set notification preferences for Announcements, go to **Categories**, then **Announcements**, and then **Enterprise Performance Management**.
2. Select **Notification preferences** and set preferences.
3. To set notification preferences for each category, navigate to the Category page and select the **Notification preferences** drop down. You must go to each Category page separately and select the **Notification preferences** drop down to set preferences.

> **Note**
>
> The **Settings and Actions** menu contains a link to Cloud Customer Connect. To open Cloud Customer Connect, from the Home page, click the down arrow next to the user name, and then select **Cloud Customer Connect**.

Turning on Accessibility Mode

In Oracle Fusion Cloud Enterprise Performance Management, users can enable Accessibility mode for all business processes, except for Enterprise Data Management which is fully accessible by default and does not require enabling Accessibility Mode.

For more information, see Enabling Accessibility in the *Accessibility Guide*.

6

Working with Clients and Tools

The client components include Oracle Smart View for Office, EPM Automate, and Financial Reporting. Availability of client components depend on your service.

In This Section:

Available Clients and Utilities

Availability of clients and utilities depends on the current Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment. For example, Oracle Smart View for Office and Financial Reporting do not apply to all clients and utilities.

You can download the following components, utilities, and templates:

- Clients for Planning, Planning Modules, and FreeForm
- Clients for Account Reconciliation
- Clients for Enterprise Profitability and Cost Management
- Clients for Financial Consolidation and Close and Tax Reporting
- Clients for Profitability and Cost Management
- Clients for Narrative Reporting
- Clients for Enterprise Data Management and Cloud EDM
- Clients for Sales Planning
- Clients for Strategic Workforce Planning

All Available Clients and Utilities

This is a list of all clients and utilities available:

- EPM Automate: EPM Automate allows Service Administrators to access environments over a command window to automate business activities such as exporting an application and downloading the exported application to desktop. See About EPM Automate in *Working with EPM Automate* for details.
- Oracle Smart View for Office: Smart View provides a common Microsoft Office interface designed specifically for Cloud EPM.
  These extensions are available in Smart View:

  - Planning Extensions: Planning Extensions include the Planning Admin Extension, which allows application administration activities, such as dimension management, to be performed from within the Excel interface; and Planning application templates, which facilitate application administration activities, such as dimension management, from within the Excel interface.
  - Smart View Add-On for Administrator: Allows application administration activities, such as dimension management, to be performed from within the Excel interface. Also referred to as the Planning Admin Extension.
  - Reconciliation Compliance Extension: Enables users to manage reconciliation compliance transactions from the Excel interface.
  - Supplemental Data Manager Extension: Enables users to perform supplemental data management from within the Excel interface.
  - Task Manager Extension: Enables users to update their tasks from within the Excel interface.
  - Enterprise Journals Extension (Financial Consolidation and Close only): Enables users to manage the data collection process and work with journals.
  - Narrative Reporting Extension: Enables users to perform assigned tasks and analyze model data from within the Microsoft Office suite.
  - EPM Books Extension: Enables users to import Books in Microsoft Excel and work with them by changing POV values and refreshing content.

- Oracle Smart View for Office (Mac and Browser): This browser-based version of Smart View is deployed in a web browser on either Windows or Mac systems for analyzing data in Microsoft Excel 365.
  These extensions are available in Smart View (Mac and Browser):
  - Admin Extension: Provides access to dimension management and application management functionality.
  - EPM Books Extension: Provides the ability to import Books in Microsoft Excel and work with them by changing POV values and refreshing content.

  See these information sources:
  - Deploying and Administering Oracle Smart View for Office (Mac and Browser): Learn about the prerequisites and how to deploy and administer Smart View in Microsoft Excel 365.
  - Working with Oracle Smart View for Office (Mac and Browser): Learn about how to connect and use Smart View features in Microsoft Excel 365 to view and analyze data.
- Oracle Smart View for Google Workspace: This browser-based version of Smart View is deployed on a web browser for analyzing data in Google Sheets.
  See these information sources:
  - Getting Started with Oracle Smart View for Google Workspace: Learn about the prerequisites and the installation information required to install Smart View in Google Sheets.
  - Working with Oracle Smart View for Google Workspace: Learn about how to connect and use Smart View features in Google Sheets to view and analyze data.
- Strategic Modeling: Strategic Modeling is an extension to Smart View that enables users to interact with Strategic Modeling, one of the Planning Modules.
- Predictive Planning: This extension to Smart View works with valid forms to predict performance based on historical data.

- Sample Content: This provides sample report packages, management reports, dimension and data load files, and a sample application for Planning Modules.

Clients for Planning, Planning Modules, and FreeForm

- EPM Automate
- Smart View for Office, Smart View for Office (Mac and Browser), and Smart View for Google Workspace
- Smart View Extensions:
  - Planning Extensions
  - Task Manager
- Predictive Planning
- Strategic Modeling (for Planning Modules only)
- Financial Reporting Web Studio

Clients for Account Reconciliation

- EPM Automate
- Smart View for Office
- Smart View Extension for Reconciliation Compliance

Clients for Enterprise Profitability and Cost Management

- EPM Automate
- Smart View for Office, Smart View for Office (Mac and Browser), and Smart View for Google Workspace
  Enterprise Profitability and Cost Management is supported only on Smart View version 22.100 or newer
- Smart View Extensions:
  - Planning Extensions
  - Task Manager

Clients for Financial Consolidation and Close and Tax Reporting

- EPM Automate
- Smart View for Office, Smart View for Office (Mac and Browser), and Smart View for Google Workspace
- Smart View Extensions:
  - Smart View Add-On For Administrator
  - Task Manager
  - Supplemental Data
  - Enterprise Journals (for Financial Consolidation and Close only)

Clients for Profitability and Cost Management

- EPM Automate
- Smart View for Office

- Financial Reporting Web Studio

Clients for Narrative Reporting

- EPM Automate
- Smart View for Office
- Smart View Extension for Narrative Reporting
- Sample Content

Clients for Enterprise Data Management and Cloud EDM

EPM Automate

Clients for Sales Planning

- EPM Automate
- Predictive Planning
- Smart View
- Planning Admin Extension
- Strategic Modeling

Clients for Strategic Workforce Planning

- EPM Automate
- Smart View
- Planning Admin Extension
- Predictive Planning

Smart View Prerequisites

The business processes must satisfy Microsoft Office requirements in addition to Oracle Smart View for Office requirements.

- The newest Smart View release is available from the Downloads tab on Oracle Technology Network. You must install the current version of Smart View to utilize the latest features.

  The current Smart View release and one prior release are supported for an Oracle Fusion Cloud Enterprise Performance Management update. For example, Smart View version 24.100 and 23.200 are supported for Cloud EPM 24.06 update.
- .NET Framework 4.8 or higher

For Smart View platform and Microsoft Office requirements, see *Smart View Support Matrix and Compatibility FAQ* (My Oracle Support Doc ID 1923582.1).

> **Note**
>
> Some services provide extensions and templates, which you download and install after installing Smart View. Extensions and templates applicable to a service are available from the **Downloads** page of the service.

To know the prerequisites for Smart View for Office (Mac and Browser) and Smart View for Google Workspace, see:

- Prerequisites in *Deploying and Administering Oracle Smart View for Office (Mac and Browser)*
- Prerequisites in *Getting Started with Oracle Smart View for Google Workspace*

Cloud EPM Business Processes Using Smart View and Calculation Manager

Smart View

Except Account Reconciliation, all Oracle Fusion Cloud Enterprise Performance Management business processes use Oracle Smart View for Office as a client component.

Calculation Manager

All Cloud EPM business processes except these use Calculation Manager:

- Account Reconciliation
- Narrative Reporting
- Profitability and Cost Management
- Tax Reporting

Downloading and Installing Clients

You can download components and utilities from the **Downloads** page, including Oracle Smart View for Office, which is available on the Oracle Technology Network.

For information on installing EPM Automate, see Installing EPM Automate in *Working with EPM Automate*.

To install clients:

1. Sign in to an environment. See Accessing Cloud EPM and Cloud EDM Environments.
2. On the **Home** page, access **Settings and Actions** by clicking your user name at the top right corner of the screen.
3. Click **Downloads**.

   The Downloads page opens. This page lists only the components applicable to the service that you are currently accessing.
4. Download the component that you want to install:

   For Smart View only:

   a. Click **Download from Oracle Technology Network**.

      The Oracle Technology Network download page is displayed.

   b. Click **Download Latest Version**.

   c. Select **Accept License Agreement**, and then click **Download Now**.

   d. If prompted to sign in, enter your Oracle Technology Network credentials and click **Sign In**.

e. Follow the on-screen instructions and save the Smart View archive to a local folder.

f. Unzip the Smart View archive to extract `SmartView.exe`.

g. Close all Microsoft Office applications.

For components other than Smart View:

a. In the **Downloads** page, click the **Download** button of the component that you want to install.

b. Follow the on-screen instructions and save the installer to a local folder.

5. Run the installer (for example, `SmartView.exe`) as an administrator.

> **Note**
>
> Before installing Smart View or any Smart View extension, close all Microsoft Office applications.
> Some Smart View extensions use the SVEXT extension. Double-click the downloaded file and follow the onscreen prompts to install it.

Accessing a Business Process Using Smart View

You can use a shared connection or a private connection to access Oracle Smart View for Office.

In this section:

Connection Types

Oracle Smart View for Office supports these connection types. You see the same data irrespective of the connection type you use.

- **Shared connections:** To connect Smart View to an Oracle Fusion Cloud Enterprise Performance Management environment, use the public URL that you would normally use to access the environment in a browser. See Configuring a Shared Connection.
- **Private connections:** Use the specific URL for the Cloud EPM environment to connect Smart View to that environment. See Configuring a Private Connection.

See Shared Connections and Private Connections in *Smart View for Office User's Guide 24.200* for more information on these connection types.

URL Syntax for Smart View Connections

Oracle Smart View for Office uses different URL syntax for shared and private connections.

Refer to Sample URLs for the Oracle Fusion Cloud Enterprise Performance Management URL pattern.

Shared Connections

In the Cloud EPM URL, replace `epmcloud` with `/workspace/SmartViewProviders` to derive the shared connection URL. For example: your shared connection URL may be `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/workspace/SmartViewProviders`.

Private Connections

You use a variation of the Cloud EPM URL pattern (see Sample URLs) to derive private connection URLs.

- **Narrative Reporting**: Replace `epmcloud` with `/epm/SmartView`. For example: your private connection URL may be `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/epm/SmartView`.
- **Profitability and Cost Management**: Replace `epmcloud` with `/aps/SmartView`. For example: your private connection URL may be `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/aps/SmartView`.
- **Planning, Financial Consolidation and Close, Enterprise Profitability and Cost Management, and Tax Reporting**: Replace `epmcloud` with `/HyperionPlanning/SmartView`. For example: your private connection URL may be `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/HyperionPlanning/SmartView`.

Configuring Connections in Smart View

After installing Oracle Smart View for Office, you must set up a connection to an Oracle Fusion Cloud Enterprise Performance Management environment.

- Configuring a Shared Connection
- Configuring a Private Connection

Troubleshooting

See Fixing Smart View Issues in the *Operations Guide*.

Configuring a Shared Connection

To configure a shared connection:

1. Start Microsoft Excel.
2. Click **Smart View**, then **Options**, and then **Advanced**.
3. In **Shared Connections URL**, enter the connection URL. See URL Syntax for Smart View Connections for connection syntax.
4. Click **OK**.

Configuring a Private Connection

See Using the Quick Connection Method in *Smart View for Office User's Guide 24* for an alternate way to create a private connection.

To configure a private connection using the Private Connection Wizard:

1. Start Microsoft Excel.
2. Click **Smart View** and then **Panel**.

3. In **Smart View Panel**, click the arrow next to (Switch to), and then select **Private Connections**.
4. Click **Create new connection** at the bottom of the panel.
5. From **Smart View**, select **Smart View HTTP Provider**.
6. In **URL**, enter the connection URL. See URL Syntax for Smart View Connections for connection syntax.
7. Click **Next**.
8. In **Login**, enter the user name and password for accessing the service, and then click **Sign In**.
9. In **Add Connection - Application/Cube**, navigate to the application and cube to work with, select it, and then click **Next**.
10. In **Add Connection - Name/Description**, enter a name for the connection and an optional description.
11. Click **Finish**.

Initiating a Smart View Connection

You may need to sign in to initiate an Oracle Smart View for Office connection.

You can connect to only one service per worksheet.

Watch this tutorial video on navigating in Smart View, including connecting to a data source.

 Tutorial Video

To initiate a connection:

1. Start Microsoft Excel.
2. Click **Smart View**, and then **Panel**.
   Choose from:
   a. Select **Shared Connections**, and then select a shared connection that you previously configured. See Configuring a Shared Connection.
   b. Select **Private Connections**, and then, from the drop-down list, select a private connection that you previously configured. See Configuring a Private Connection.
3. Click (Go to the selected Server or URL).
   The **Login** screen is displayed.
4. In **Login**, enter the user name and password for accessing the service, and then click **Sign In**.

Troubleshooting

See Fixing Smart View Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Connecting to a Business Process Using Financial Reporting Web Studio

You access Financial Reporting Web Studio by selecting a link from an environment.

To launch Financial Reporting Web Studio:

1. Using a browser, access an Oracle Fusion Cloud Enterprise Performance Management environment. See Accessing Cloud EPM and Cloud EDM Environments.
2. Click  (Navigator), and then select **Reporting Web Studio**.

7

Managing Users and Groups in OCI IAM

User and group management can be configured in several ways, depending on your organization's identity setup:

- **Directly in the IAM Interface in Oracle Cloud Console:** Create and manage users and groups through the Identity and Access Management (IAM) interface. See:
  - Creating User
  - Updating User
  - Deleting Users
- **Through an external Identity Provider (IdP):** Integrate with providers such as Microsoft Entra ID or Okta using SAML 2.0 federation. Authenticated users are automatically synchronized with IAM for centralized access management. See Using SCIM to Synchronize Users and Groups on Oracle Identity Cloud.
- **Group Memberships:** Users can be added directly to IAM (IDCS) groups or automatically synced from enterprise IdP groups. See Creating IDCS Groups.
- **Policies:** Assign policies to groups to provide fine-grained control over the actions and permissions available to each set of users. See Setting Password Policies.

About User and Role Management

The environment is protected by multiple layers of security. Oracle implements and manages infrastructure security components to create highly secure Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. Access is restricted to authorized users through various mechanisms, including:

- Single Sign-On (SSO)
- Role-based access to environments

Both SSO and role-based security are governed by Oracle Identity Management, which establishes a security domain for each environment. After a successful signin, access to the service is determined by the role assigned to the user.

Cloud Account Name

The Cloud Account Name is the Oracle account that manages your subscription. In OCI (Gen2), Identity Domain Administrators use IAM Interface in Oracle Cloud Console to set up and manage users and security.

The Account Administrator grants the Identity Domain Administrator role to one or more users to delegate security setup responsibilities. By default, each customer is allocated two environments: one for testing and other for production. Multiple services may be activated under one cloud account.

Users

Each user who needs to access an environment must have an account in the identity domain associated with the environment. The predefined roles assigned to the user determine what the user can do within an environment.

Predefined Cloud EPM Roles

Roles link users to the business activities that they are permitted to perform within an environment and the data that they can access. Users must be assigned to predefined roles that grant them access to business functions and associated data. Predefined roles are described in Understanding Predefined Roles. Identity Domain Administrator is not a predefined role.

Groups

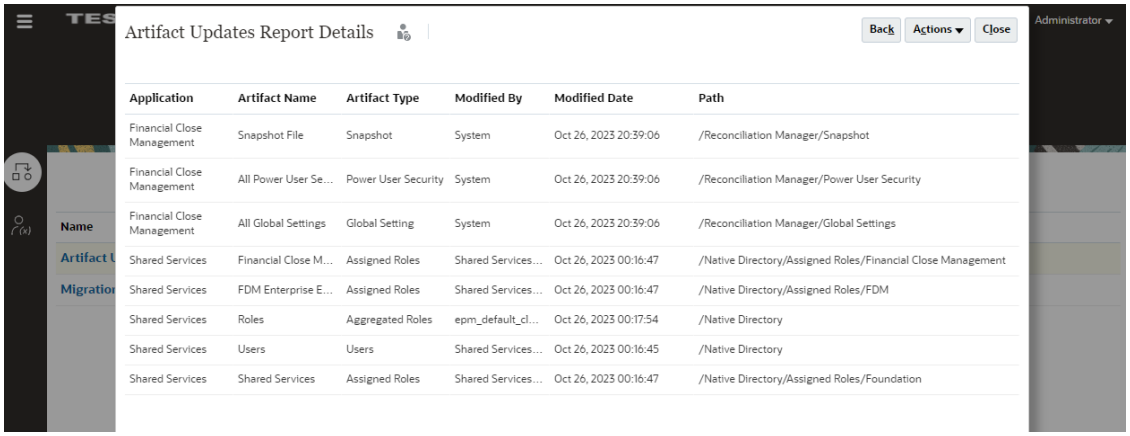
There are three types of groups:

- PREDEFINED: These groups are automatically created for each predefined role. All users are assigned to a PREDEFINED group based on their predefined role (for example, Power User). You can view them in Access Control.
- EPM: These are the groups that you create in Access Control. They cannot be created in Oracle Cloud Console.
- IDCS: In OCI (Gen2), multiple users can be assigned to groups, which can then be assigned predefined roles. This eliminates the need to assign predefined roles to individual users, simplifying role administration. Since Oracle Identity groups can be synced with identity provider (IdP) groups (such as Microsoft Entra ID), you can add individual users to IdP groups and assign predefined roles to these groups in the IAM Interface of Oracle Cloud Console. These groups can also be synchronized with identity providers like Okta or Microsoft Entra ID. Although they will appear in Access Control, they cannot be created directly through this interface.

Use of SYSTEM as a Username

The environment shows the user name as SYSTEM if there are changes done internally or it is not recorded who made the change. There is no real user on the environment with this name. For example, for the following Account Reconciliation artifacts, there may be many **Modified By** users or the **Modified By** user is not always recorded. In such cases, SYSTEM is identified as the **Modified By** user:

- Snapshot
- Aging Profile
- Currency Bucket
- Global Settings
- Power User Security
- Rate Type



Related Tutorial

This tutorial describes the layers of security in business processes and shows you how to manage security using Access Control and access permissions. The sections build on each other and should be completed sequentially. See Setting Up Security in Cloud EPM Business Processes.

Understanding Predefined Roles

Most services use a common set of predefined functional roles to control access to environments. Once you have been migrated to the environment, your legacy roles are mapped to the corresponding predefined role.

Access to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments is granted by assigning users to predefined roles. For example, to permit user `John Doe` to view reports belonging to a Planning test environment, he should be assigned to the Viewer role of the environment.

All Cloud EPM business processes, except for Enterprise Data Management, use a common set of four predefined functional roles to control access to environments.

- Service Administrator
- Power User
- User
- Viewer

Cloud EDM and Enterprise Data Management specifically use Service Administrator and User roles.

The level of access granted by each predefined role varies depending on the service type. For example, the Power User role in Planning enables you to manage business rule security and control the approval process while the same role in Tax Reporting enables you to run tax automation and import data.

> **Note**
>
> The behavior of all predefined roles other than Service Administrator is affected by the **Apply Security** option defined at the dimension level in the business process. Disabling the **Apply Security** option leaves dimensions unsecured allowing all users assigned to predefined roles to access and write data to dimension members. Oracle recommends that you select the **Apply Security** option at the dimension level to enforce security.

Predefined functional service roles are hierarchical. Access granted through lower-level roles is inherited by higher-level roles. For example, Service Administrators, in addition to the access that only they have, inherit the access granted through Power User, User, and Viewer roles.

Account Reconciliation

Service Administrator

Configures the system and manages the worldwide reconciliation process. These users have unrestricted access to all Account Reconciliation features including the ability to view all reconciliations.

Power User

Adds and maintains profiles and creates reconciliations from those profiles, but only if the profiles fall within the user's security filter. A Service Administrator defines security filters from the **System Settings** configuration tab of the Account Reconciliation environment.

Generally, this role is assigned to users who have regional reconciliation management responsibilities.

Power Users can administer authorized sets of profiles and reconciliations in Account Reconciliation. This feature is designed for companies with distributed reconciliation processes that require participation of employees familiar with configuring profiles and reconciliations locally.
Authorization of profiles and reconciliations occurs through security filters on account segments. For example, Power User A might be granted authorization only to profiles or reconciliations where segment one = 100 and segment two starts with 12. Security filters are created and assigned to each Power User.

User

Prepares and reviews account reconciliations or views or comments on reconciliations. Access to reconciliations is controlled by the assignment of the user to the reconciliation. For example, in order to prepare a given reconciliation, the user must be assigned the Preparer role for that reconciliation.

Typically, this role is granted to preparers, reviewers, and commentators on reconciliations.

Viewer

Views reconciliations.

Enterprise Profitability and Cost Management

Service Administrator

Performs all functional activities in an environment.

This role should be granted to functional experts who need to create and administer Enterprise Profitability and Cost Management application and service components.

Power User

Drives the model development and execution process. This role grants high-level access to several functional areas within an environment and should be granted to the lead modelers and integrators working with the model, and business users in charge of a region who need to control the calculation process.

Power Users can perform all the activities that a User can perform. Additionally, a Power User can perform these tasks:

- Creates ad hoc grids and writes back into ad hoc grids, creates and maintains Reports and Financial Reporting reports, and loads data using Data Integration
- Creates, clears, and copies POV data
- Creates and runs integrations
- Creates models
- Creates and edits profit curve
- Updates metadata and performs all application management tasks except creation and deletion

User

Enters data where user input is requested, runs analytical tools and reports, and designs rules and calculations. Users can perform all the tasks that Viewers can perform. A User can perform these additional operations:

- Performs ad hoc functions, but cannot write back into ad hoc grids or load data using Data Integration
- Performs drill through
- Creates, modifies, and deletes rules
- Performs mass edits of rules
- Runs rule balancing
- Runs validations
- Runs calculations, views and deletes calculation history
- Previews Reports and Books

Viewer

Views and analyzes data but does not have write access. Specifically, a Viewer performs these operations:

- Runs profit curve
- Runs trace allocation

- Views models
- View the information in the following components:
  - Valid Intersections
  - Data Exchanges
  - Jobs
  - Task Manager

Financial Consolidation and Close

Service Administrator

Performs all Financial Consolidation and Close functional activities, including granting roles to users.

- Access all tasks, Task Manager templates and schedules
- Create and manage Task Types, Integration Types, Attributes, and Alert Types
- Generate and manage Task Manager and Supplemental Data Manager reports
- Define and deploy Supplemental Data sets, and manage data collection periods
- Manage Supplemental Data forms

This role should be granted to Financial Consolidation and Close experts who need to create and administer the Consolidation application and service components.

Power User

Views and interacts with data. This role grants high-level access to several Financial Consolidation and Close functional areas and should be granted, typically, to the consolidation experts and regional senior financial analysts of your organization. A Power User can perform these activities:

- Create and maintain forms, Oracle Smart View for Office worksheets, business rules, task lists, Reports, and Financial Reporting reports
- Consolidate data as needed for entities to which they have access
- Control the approvals process, perform actions on consolidation units and journals to which they have modify access, and assign owners and reviewers for the organization under their charge
- Import data
- Create and save Smart Slices
- Create and manage Task Manager tasks, templates, Task Types, and schedules
- Define and deploy Supplemental Data sets
- Define Supplemental Data forms and modify form data

> **Note**
>
> Anyone other than a user with the Viewer role can become an owner or reviewer.

User

The activities that a User can perform includes:

- Enter and submit data for approval, analyzes forms using ad hoc features, and control the ability to drill through to the source system. Create and submit for approval the journals for dimension members for which they have Modify rights
- Access Data Management (to create an integration, run an integration, and drill through) and load data if an application role that grants such access is assigned to the user
- Modify task status, create and modify Task Manager alerts, comments, and questions
- Access Task Manager and Supplemental Data Manager Dashboards
- Enter and edit data in Supplemental Data forms
- Previews Reports and Books

Viewer

Tasks that a Viewer can perform includes:

- View and analyze data through forms and any data access tool, such as reports, Smart Slices, and journals if the user is granted access rights to related objects such as data forms and ad hoc grids (the user cannot create these objects). A user with only View access cannot access Consol or Rates cube
- View Task Manager schedules and Supplemental Data form data

This role typically should be assigned to executives who need to view consolidation and close reports.

FreeForm and Planning

These predefined roles apply to FreeForm and Planning business processes, as well as all Planning application types, including Custom, FreeForm , Planning Modules, Predictive Cash Forecasting, Strategic Workforce Planning, and Sales Planning.

Service Administrator

Performs all Planning functional activities, including granting roles to users. This role should be granted to functional experts who need to create and administer Planning business process components.

Power User

Views and interacts with data. This role grants high-level access to several functional areas within an environment and should be granted to department heads and business unit managers, and business users in charge of a region who need to control the approval process.

A Power User can perform these activities:

- Creates and maintains forms, Oracle Smart View for Office worksheets, Reports, and Financial Reporting reports
- Creates and manages user variables for the application, but cannot delete them.
- Views substitution variables
- Controls the approvals process, performs actions on approval units to which they have write access, and assigns owners and reviewers for the organization under her charge

- Creates Reports using Financial Reporting, accesses the repository to create folders and save artifacts
- Loads data using forms and Data Management

User

The Planner legacy role is assigned to User in OCI (Gen2) environments.

> **Note**
>
> The User role was created by renaming the Planner role. If your service was provisioned after May, 2016, you will see the User role and not the Planner role.

A User does the following:

- Enters data into forms and submits them for approval, analyzes forms using ad hoc features, controls the ability to drill through to the source system
- Accesses and modifies (rename, delete) the Financial Reporting content stored in the Repository for which the user has View, Modify, or Full Control permissions.
- Previews Reports and Books

Viewer

Views and analyzes data through forms and data access tools. Typically, this role should be assigned to executives who need to view business plans during the budgeting process.

Profitability and Cost Management

Service Administrator

Performs all functional activities in an environment.

This role should be granted to functional experts who need to create and administer Profitability and Cost Management application and service components.

Power User

Views and interacts with data. This role grants high-level access to several functional areas within an environment and should be granted to department heads and business unit managers, and business users in charge of a region who need to control the approval process.

A Power User can perform activities including the following:

- Adds allocation rules, analytical features, financial reports, and queries
- Imports and exports data
- Calculates application models
- Runs calculation jobs
- Updates metadata and performs all application management tasks except creation and deletion

User

- Enters data where user input is requested

- Runs analytical tools and reports
- Designs reports, queries, dashboards, and other analytical elements
- Users with this role cannot calculate data or run calculation jobs

Viewer

- Views and analyzes data but does not have write access
- Viewers with this role cannot calculate data or run calculation jobs

Oracle Enterprise Data Management

Service Administrator

Performs all Oracle Enterprise Data Management functional activities such as creating applications, views and updating data. Performs administrative tasks including granting functional roles to users, migrating artifacts across test and production environments, and performing daily maintenance.

This role should be granted to functional experts who need to create and administer Oracle Enterprise Data Management applications and data.

User

A user in Oracle Enterprise Data Management can be assigned roles to create views and applications and assigned permissions to work with applications, views and data chains.

> **Note**
>
> **Power User** and **Viewer** predefined roles are also displayed in IAM Interface of Oracle Cloud Console. Do not assign users to these roles, which are not applicable to Oracle Enterprise Data Management.

Narrative Reporting

Service Administrator

Performs all functional activities, including granting predefined roles to Narrative Reporting users.

Power User

- Creates report packages, management reporting definitions, and Reports.
- Creates folders, including root-level folders.
- Creates and maintains all artifacts, such as models, dimensions, and data grants.

User

- Views Narrative Reporting artifacts to which the user has access
- Previews Reports and Books

Viewer

Views reports and other artifacts to which the user has access. This is the minimum role required to sign in to and use an environment.

> **Note**
>
> The Narrative Reporting legacy roles are not available in OCI (Gen2) environments and are assigned to the following predefined roles:
>
> - System Administrator to Service Administrator
> - Library Administrator, Application Administrator, and Report Administrator to Power User

Tax Reporting

Service Administrator

Performs all functional activities (read, write, and update) in Tax Reporting, including granting roles to users, and metadata and data, for all entities or a specific group or entity. This role also performs tax automation.

This role should be granted to Tax Reporting experts who need to create and administer the application and service components.

- Accesses all tasks, Task Manager templates and schedules
- Creates and manages Task Types, Integration Types, Attributes, and Alert Types
- Generates and manages Task Manager and Supplemental Data Manager reports
- Defines and deploys Supplemental Data sets, and manage data collection periods
- Manages Supplemental Data forms

Power User

Views and interacts with data. This role grants high-level access to several Tax Reporting functional areas and should be granted, typically, to the consolidation experts and regional senior financial analysts of your organization. A Power User can perform these activities:

- Reads and writes to the application, runs tax automation, and imports data for the assigned entities.
- Create and maintain forms, Oracle Smart View for Office worksheets, business rules, task lists, Reports, and Financial Reporting reports
- Imports data
- Creates and saves Smart Slices
- Creates and manages Task Manager tasks, templates, Task Types, and schedules
- Defines and deploys Supplemental Data sets
- Defines Supplemental Data forms and modifies form data

> **Note**
>
> Anyone other than a user with the Viewer role can become an owner or reviewer.

User

The activities that a User can perform includes the following:

- Reads, writes, and updates only tax-related forms for the assigned entities. Also, enters and submits data for approval, analyzes forms, consolidates data, and creates and submits journals for dimension members to which they have access. This role cannot perform tax automation.
- Accesses Data Management (to create an integration, run an integration, and drill through) and load data if an application role that grants such access is assigned to the user
- Modifies task status, create and modify Task Manager alerts, comments, and questions
- Accesses Task Manager and Supplemental Data Manager Dashboards
- Enters and edits data in Supplemental Data forms
- Previews Reports and Books

Viewer

Tasks that a Viewer can perform include the following:

- Views reports and has read-only access to specified forms to view and analyze data through forms and any data access tools. Data Access tools include reports, Smart Slices, journals, and ad hoc grids. This access is usually assigned to reviewers, directors, executives, and so on
- Views Task Manager schedules and Supplemental Data form data

Domain-Level Administrator Roles

In addition to the predefined roles that are assigned to the users in each environment, there are administrator roles at the domain-level. These roles are described below :

Domain Level Administrator Role	Privileges
Identity Domain Administrator	Has super user privileges for an identity domain in Identity Cloud Service. Identity Domain Administrator can: • manage users, groups, applications, system configuration, and security settings • enable and disable Multi-Factor Authentication (MFA), configure MFA settings, and configure authentication factors • create self-registration profiles to manage different sets of users, approval policies, and applications Any user assigned to the Identity Domain Administrator role can manage users and predefined role assignments in the environment. Such users can also view User Login report as well as Role Assignment Audit report. Identity Domain Administrator can execute these EPM Automate commands as long as they also have a predefined role assigned to them : • addUsers • removeUsers • updateUsers • assignRole • unassignRole • roleAssignmentAuditReport • invalidLoginReport Identity Domain Administrator can execute these REST APIs as long as they also have a predefined role assigned to them: • Add Users to an Identity Domain • Remove Users from an Identity Domain • Update Users • Assign Users to a Predefined Role • Remove Users' Role Assignment • Role Assignment Audit Report for OCI • Invalid Login Report for OCI The Identity Domain Administrator can delegate some of their responsibilities to other users that have one of the roles listed in the rows below.
Security Administrator	Can manage Oracle Identity Cloud Service system configuration and security settings for an identity domain. Security Administrator can customize the interface, default settings, notifications, and the password policies, configure MFA, and manage the Microsoft Active Directory (AD) Bridge, Provisioning Bridge, identity providers, and trusted partner certificates.
Application Administrator	Can create, update, activate, deactivate, and delete applications. Application administrators can also grant and revoke access to applications for groups and users. The Application Administrator cannot execute assignRoles or unassignRole EPM Automate command, or the corresponding Assign Users to a Predefined Role or Remove Users' Role Assignment REST API.
User Administrator	Can manage users, groups, and group memberships for an identity domain. The User Administrator cannot execute addUsers, removeUsers, or updateUsers EPM Automate command, or the corresponding Add Users to an Identity Domain, Remove Users from an Identity Domain, or Update Users REST API.

Domain Level Administrator Role	Privileges
User Manager	Can manage all users or users of selected groups in Oracle Identity Cloud Service. User managers can update, activate, deactivate, remove, and unlock user accounts. User managers can also reset passwords, reset authentication factors, and generate bypass codes for user accounts. The User Manager cannot execute removeUsers or updateUsers EPM Automate command, or the corresponding Remove Users from an Identity Domain, or Update Users REST API.
Help Desk Administrator	Can manage all users or users of selected groups in Oracle Identity Cloud Service. Help desk administrators can view the details of a user and unlock a user account. Help desk administrators can also reset passwords, reset authentication factors, and generate bypass codes for user accounts.
Audit Administrator	Can run reports for an identity domain in Oracle Identity Cloud Service. The Audit Administrator cannot execute roleAssignmentAuditReport or invalidLoginReport EPM Automate command, or the corresponding Role Assignment Audit Report for OCI or Invalid Login Report for OCI REST API.

The administrators can use the IAM Interface of Oracle Cloud Console to manage their privileges listed above.

> **Note**
>
> - Service Administrators can assign or unassign predefined roles to the user without being assigned to the Identity Domain Administrator role. To allow only Identity Domain Administrator to assign predefined roles, you can send a request to Oracle. For details, see Requesting to Disallow Service Administrators to Assign Predefined Roles in OCI(Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide*.
> - A user who is assigned only to a domain-level administrator role is not counted in the Named Users license count. Only the users assigned to the predefined roles are included in the Named Users license count.

Managing Users

Any user assigned to the Identity Domain Administrator role can manage users and predefined role assignments in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. If you create users but not assign them to predefined roles, then they will not appear in the environment. Any predefined role assignment or unassignment is reflected in Access Control only after one of the following conditions occur:

- A user logs in after 4+ minutes approximately.
- When a user access Role Assignment Report tab in Access Control.
- An EPM Automate `assignRole` or `unassignRole` or `roleAssignmentReport` command is executed
- The REST API for assign role, unassign role, or role assignment report is executed

If the users and pre-defined role assignments are imported using EPM Automate `importSnapshot` or `cloneEnvironment` commands or REST API, the changes are reflected in Access Control immediately.

See Assigning Roles to Users.

Troubleshooting

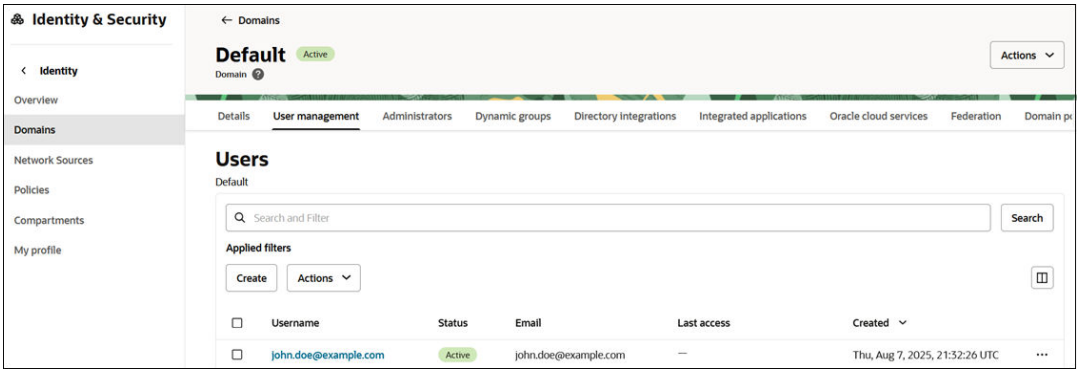
See Resolving User, Role, and Group Management Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Creating User

Identity Domain Administrators can create users individually or use an upload file containing user data to create many users at once. They should be proficient in security concepts, including predefined roles that allow users to gain access to an environment.

To create a user:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to **User management** tab.



3. Click **Create**.
4. On **Create user** page, enter the required user information. The username can be a maximum of 256 characters.
5. You can also select groups to assign to this user.

> **Note**
>
> If you are creating a user who can add subscriptions to an existing Oracle Cloud Account, be sure to select the **Administrators** group.

6. Click **Create**. An email notification is sent to the new user.

> **Note**
>
> Each user has a Recovery email that you can add by editing the user information.

You can also create a user using REST API and EPM Automate command. Refer to the links below:

- Add Users to an Identity Domain in *REST APIs*
- addUsers in *Working with EPM Automate*

To create multiple users at once, refer to the links below:

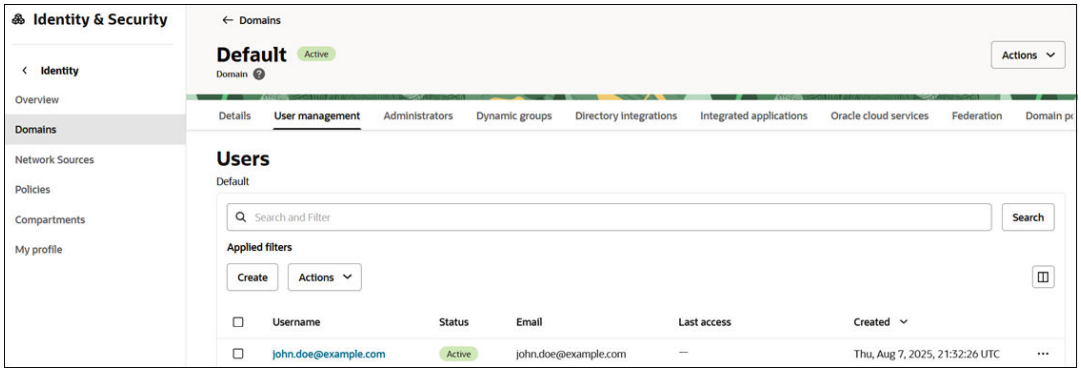
- addUsers in *Working with EPM Automate*
- Import User Accounts in *Administering Oracle Identity Cloud Service*

Creating IDCS Groups

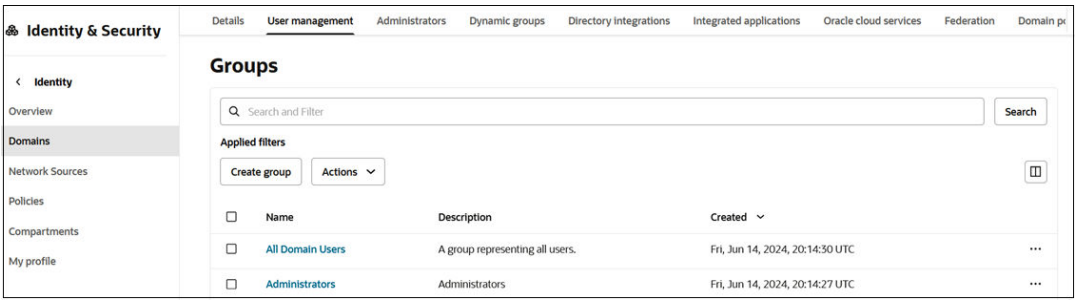
You can create an IDCS group and assign users to it, making it easier to manage policies and permissions. Additionally, you can assign predefined roles to multiple users simultaneously using IDCS groups, simplifying access management.

To create a group:

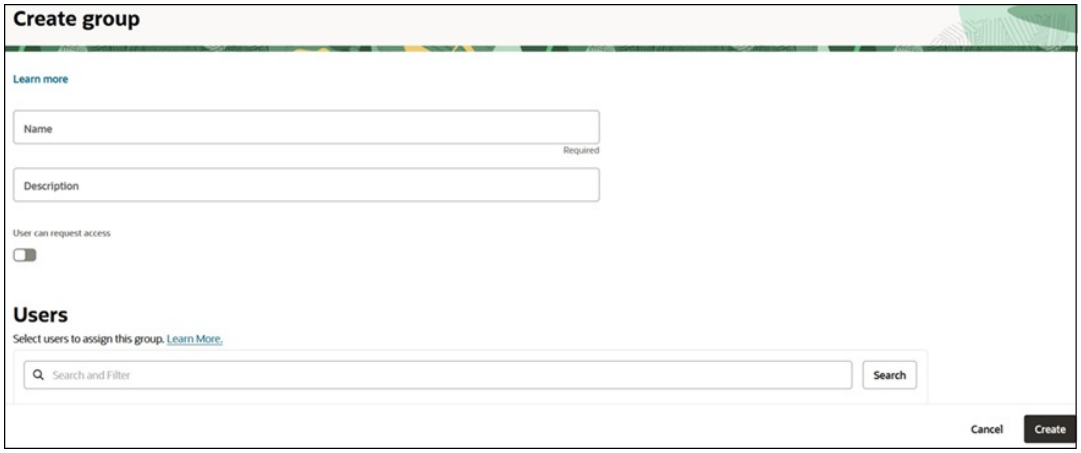
1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to **User management** tab.



3. Scroll down to **Groups** section.



4. Click **Create group**.
5. On **Create group** page, enter group information.
6. To add users to the group, search and select the users that you want to add to the group.
7. Click **Create** to create this group. The new IDCS group is now added in the Groups page.



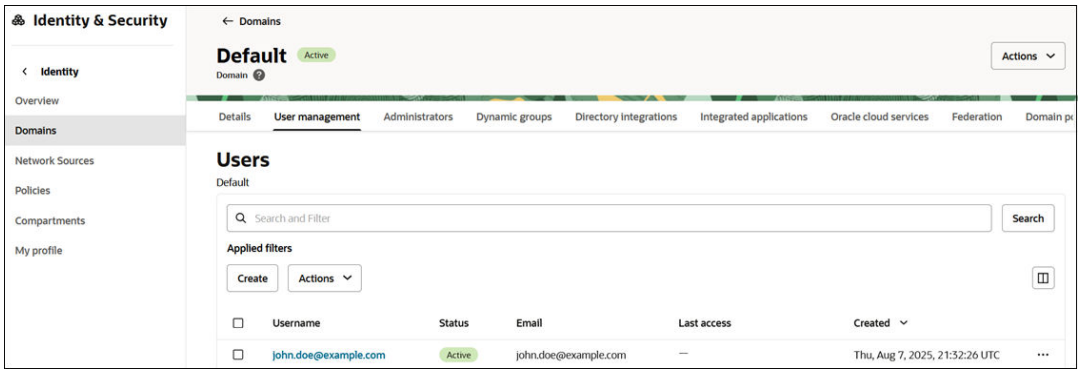
Updating User

Identity Domain Administrators can modify the users' first and last names. If the user's email address is used as their username, you must delete and re-add the user to update the email address or username. If the email address is not the username, you can modify the email address but not the username.

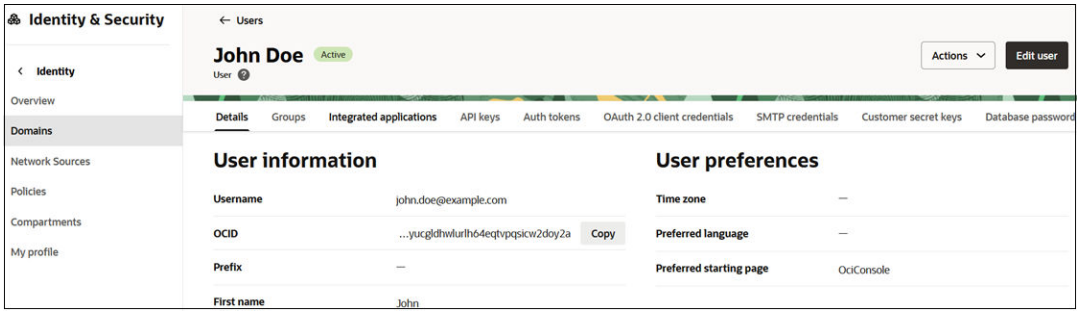
In the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments, only the user's primary email address is displayed, and any available recovery email address is not shown. However, the recovery email address is visible in the IAM Interface. You can update the recovery email address by editing the user's information. This update is not possible via EPM Automate or REST API.

To edit the user information:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to **User management** tab.



3. Click the **Username** from the list below.
4. On this user's page, click **Edit user.**



5. Update the user information and click **Save changes**.
   Changes to the first name, last name, and email ID (if not used as the username) will be reflected about five minutes after the user logs in.

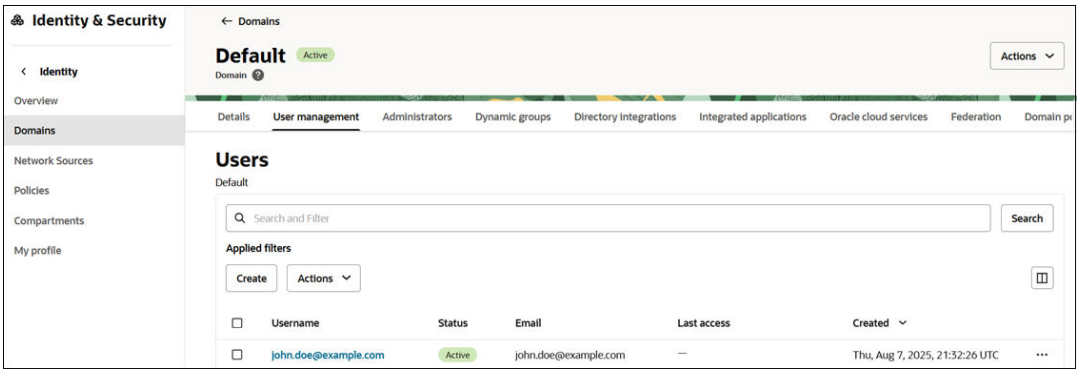
You can also update the user information using REST API and EPM Automate command. Refer to the links below:

- Update Users in *REST APIs*
- updateUsers in *Working with EPM Automate*

Deleting Users

To delete a user:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to **User management** tab.



3. Search and select the users to delete from the list below.
4. Click **Actions** under **Applied fiters**, and then select **Delete**.

You can also delete users using REST API and EPM Automate command. Refer to the links below:

- Remove Users from an Identity Domain in *REST APIs*
- removeUsers in *Working with EPM Automate*

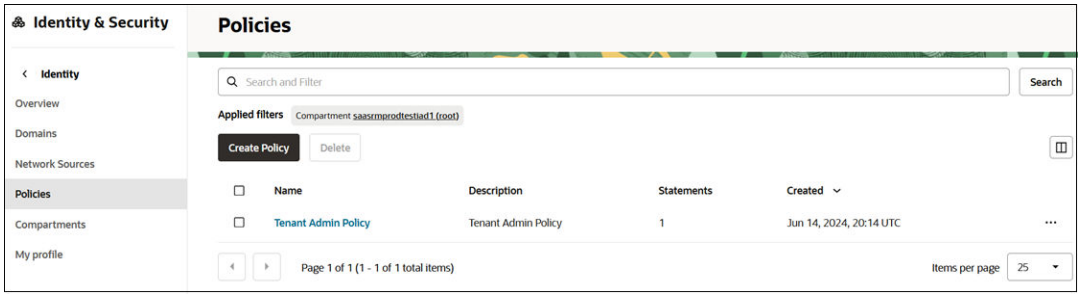
Creating Policies for Users and Groups

Policies can be assigned to groups to enable granular control over the actions each group of users can perform. By default, access to Oracle Cloud Console is restricted to Cloud Account Administrators and Identity Domain Administrators. Service Administrators of individual environments must be assigned the appropriate policies to be able to view those environments in the Oracle Cloud Console. Similarly, users must be assigned to specific policies to view notifications.

You have the flexibility to create multiple groups, each with its own policy, and assign users accordingly. This enables granular control over the actions that each group of users can perform.

To create a policy:

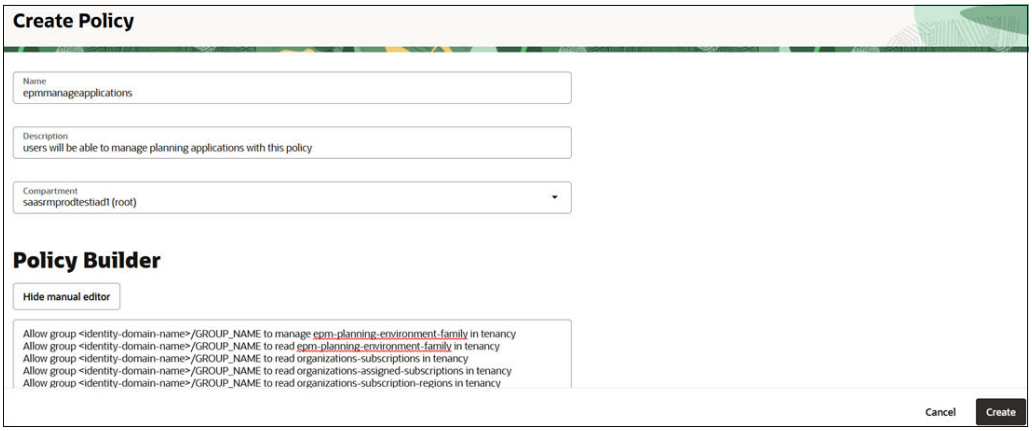
1. (Optional) If needed, create the users and groups to whom you want to assign policies. See:
   - Creating User
   - Creating IDCS Groups
2. Go to the **Navigation** menu, search for *Identity*, and select **Policies**.
3. Select the **Compartment** for which you are defining the policy.



4. Click **Create Policy** to create the necessary read and manage policies.
   a. In Create Policy, enter a **Name** and a **Description** for the policy.
   b. Select the **Compartment**.
   c. In **Policy Builder**, enter policy statements.
   Be sure to replace *GROUP_NAME* with the name of the group to which you want to apply the policy. For example:

```
Allow group <identity-domain-name>/GROUP_NAME to manage epm-planning-
environment-family in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read epm-planning-
environment-family in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
subscriptions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
assigned-subscriptions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read organizations-
subscription-regions in tenancy
Allow group <identity-domain-name>/GROUP_NAME to read app-listing-
environments in tenancy
```

```
Allow group <identity-domain-name>/GROUP_NAME to read metrics in tenancy
Allow group <identity-domain-name>/GROUP_NAME to inspect domains in
tenancy
Allow group <identity-domain-name>/GROUP_NAME to read announcements in
tenancy
```



5. Click **Create**.

Assigning Roles to Users

If you create users but not assign them to predefined roles, they will not be reflected in the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environment. You can assign predefined roles to users while creating them or later on by loading user assignments to role from a CSV file. You can also use identity groups to assign predefined roles to multiple users.

Any user assigned to the Identity Domain Administrator role can manage users and predefined role assignments in the environment. Service Administrators can assign or unassign predefined roles without being assigned to the Identity Domain Administrator role. See Understanding Predefined Roles for detailed information on predefined roles.

See these topics:

- Assigning Roles
- Using IDCS Groups to Assign Predefined Roles to Users
- Assigning Roles Using CSV files

Users that have not been assigned to a predefined role are considered as deactivated users.

Any predefined role assignment or unassignment is reflected in Access Control only after one of the following conditions occur:

- A user logs in after 4+ minutes approximately.
- When a user access Role Assignment Report tab in Access Control.
- An EPM Automate `assignRole` or `unassignRole` or `roleAssignmentReport` command is executed
- The REST API for assign role, unassign role, or role assignment report is executed

If the users and pre-defined role assignments are imported using the `importSnapshot` or `cloneEnvironment` EPM Automate commands or REST API, the changes are reflected in Access Control Immediately.

> **Note**
>
> After assigning roles, a Service Administrator should email users the URLs for accessing the test and production environments of the service. Remember that different URLs are used for the test and production environments, so be sure to include the correct one in the email.

Assigning Roles Using CSV Files

To assign predefined roles to many users at once, you use role upload files, one for each role. Create role upload files by dividing the users in the user upload file among comma-separated value files, one for each role. Each file must contain the user name of the users to whom you want to assign a specific role.

> **Note**
>
> The environment does not support the use of custom roles created in the identity domain.

Email Notification to User

By default, the Cloud Account Administrator (`oraclecloudadmin_ww@oracle.com`) sends an email to each new user after the user is assigned a predefined role.

The email contains the credentials (user name and a temporary password) that the user needs to sign in to the environment.

- User names must contain only ASCII characters and must be unique within the identity domain.
- If used as the user name, the Email ID must be unique.
- The first name, last name and email ID of users may contain the apostrophe punctuation mark (').
- Email IDs containing the apostrophe punctuation mark cannot be used as the user name.

> **Note**
>
> In case the user is assigned a predefined role using groups, this email notification will not be sent.

Troubleshooting

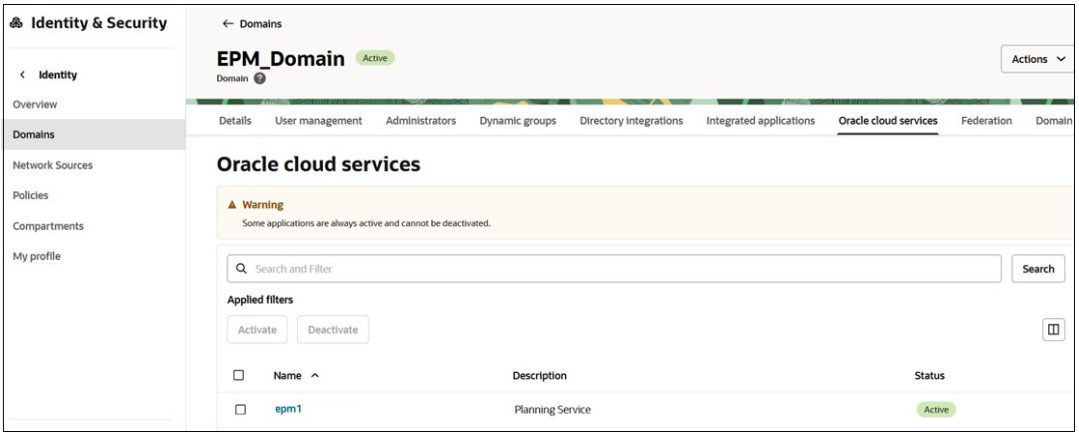
See Resolving User, Role, and Group Management Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Assigning Roles

Assign predefined roles to your users in IAM Interface.

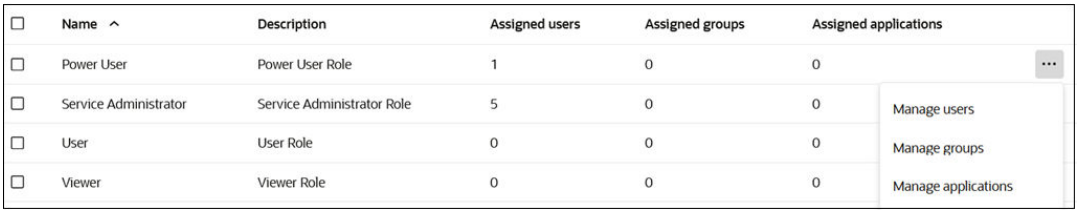
To assign roles to users:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Click **Oracle Cloud Services** tab.
   A list of available Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments is displayed.
3. Click the name of the environment for which you want to assign predefined roles to users.

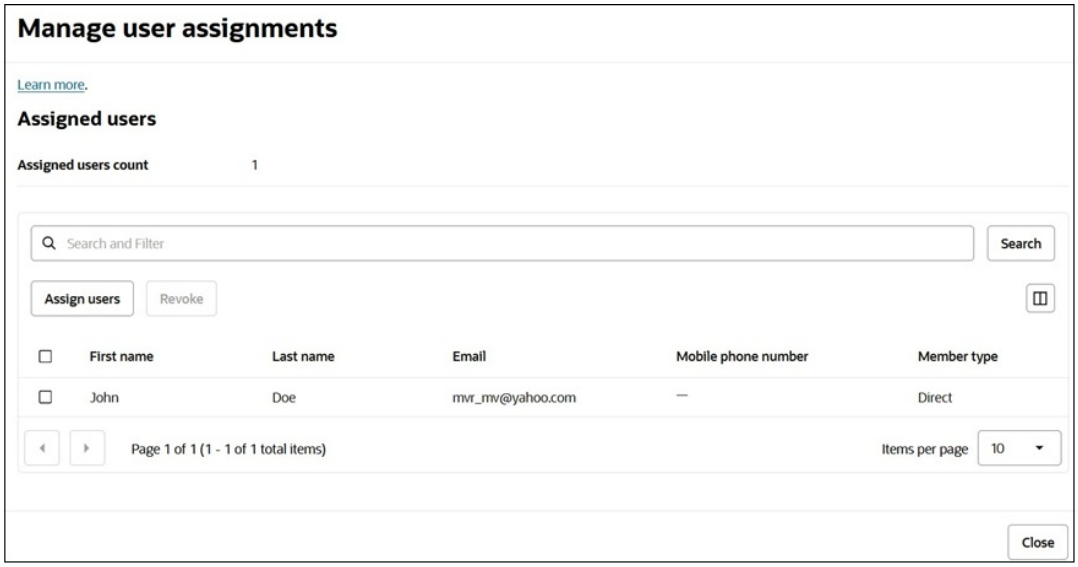


4. Click **Application Roles** tab.

5. Click the **ellipses** next to the role you want to assign and select **Manage users**.



6. On Manage user assignments page, click **Assign users**.



7. Search and select the users you want to assign to the current predefined role.
   To search for a user, click the text box, enter all or part of the beginning of the user name, first name, or last name of the user, and then press **Enter**.
8. Click **Assign**.
   Since you directly assigned users to the predefined role, they are listed as Direct Member type.

You can also assign roles to a user using REST API and EPM Automate command. Refer to the links below:

- Assign Users to a Predefined Role or Application Role in *REST APIs*
- assignRole in *Working with EPM Automate*

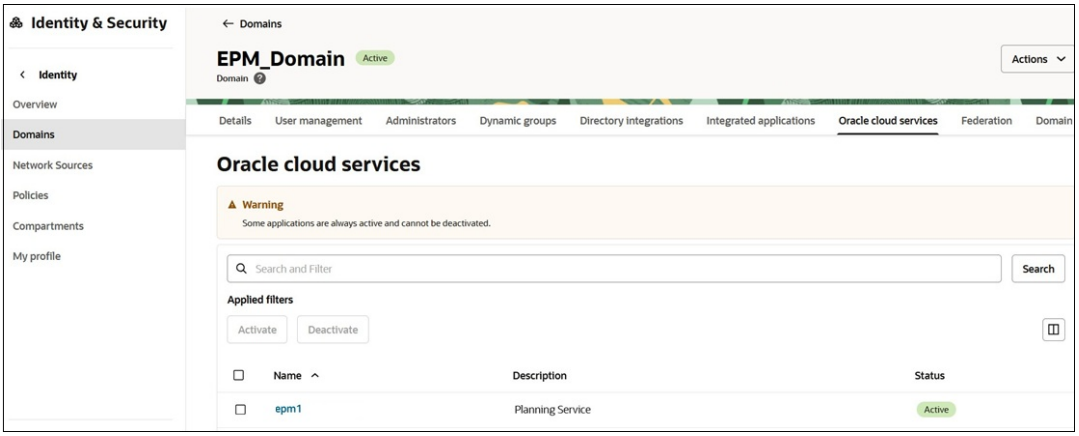
Using IDCS Groups to Assign Predefined Roles to Users

You can use Identity groups to assign predefined roles to multiple users. Since Identity groups can be synced with identity provider (IdP) groups (such as Entra ID groups), you can even add individual users to IdP groups and assign the predefined roles to these groups in IAM Interface.

> **Note**
>
> Renaming an Identity group is functionally equal to deleting it and creating a new one.

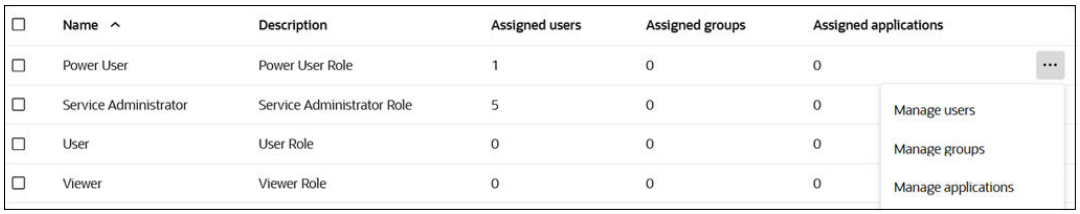
To assign groups to a predefined role:

1. Click **Oracle Cloud Services** under **Identity Domain**.
   A list of available environments is displayed.

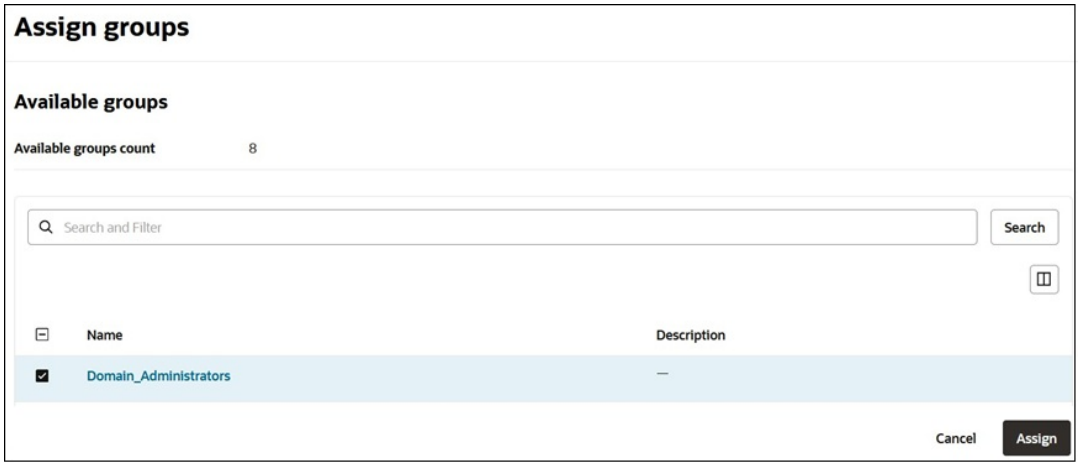


2. Click the name of the environment for which you want to assign predefined roles to users.
3. Click **Application Roles** tab.

4. Click the **ellipses** next to the role you want to assign and select **Manage groups**.



5. On the **Manage group assignments** page, click **Assign groups**.
6. On the **Assign groups** page, select the groups you want to assign to the current predefined role.
   To search for a user, click the text box, enter all or part of the beginning of the user name, first name, or last name of the user, and then press **Search**.
7. Click **Assign**.



When you clone an environment with the option to clone users and predefined roles, the cloned users on the target environment will have the predefined roles assigned to them directly, even if they are assigned through IDCS groups. See Cloning EPM Cloud Environments in *Administering Migration for Oracle Enterprise Performance Management Cloud*.

Unassign Roles

Identity Domain Administrators can, by unassigning a role, deny access that was previously granted. You unassign a role by modifying the roles assigned to the users.

You can also unassign roles to a user using REST API and EPM Automate command. Refer to the links below:

- Remove Users' Role Assignment in *REST APIs*
- unassignRole in *Working with EPM Automate*

Using SCIM to Synchronize Users and Groups on Oracle Identity Cloud

The System for Cross-domain Identity Management (SCIM) provides a standardized mechanism for automating the exchange of user and group identity information between services. Within Oracle Cloud, SCIM is utilized to enable synchronization of identity objects across the following:

- **Across Oracle Cloud services deployed in separate identity domains (same or different cloud accounts)**. For example, syncing users and groups from Fusion ERP to Oracle Fusion Cloud Enterprise Performance Management. See Synchronizing Users and Groups Across Identity Domains (Same or Different Cloud Accounts).
- **With third-party identity providers such as Microsoft Entra ID**. See Synchronizing Users and Groups from Microsoft Entra ID to IAM.

Synchronizing Users and Groups Across Identity Domains (Same or Different Cloud Accounts)

Follow the step-by-step instructions in the links provided to synchronize either all, or specific users or groups:

- Synchronization Steps for All Users and Groups Using the IAM Interface
- Synchronizing Specific Users and Groups in IAM Interface

Synchronization Steps for All Users and Groups Using the IAM Interface

To synchronize all users and groups from a source domain to a target domain (within the same cloud account or across separate cloud accounts), follow the step-by-step instructions in the provided links:

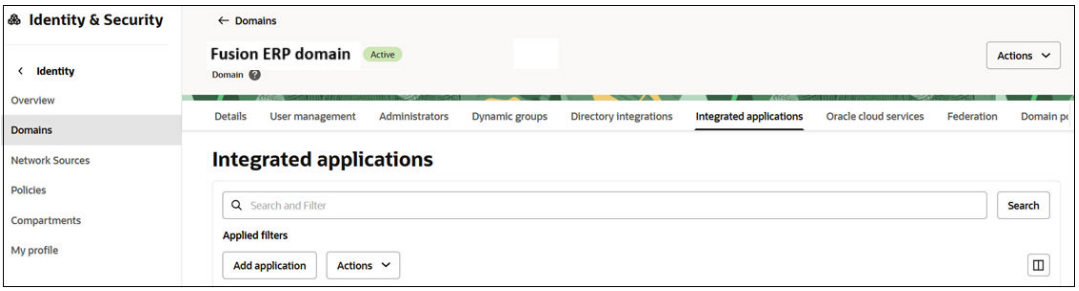
For example, if Oracle Fusion Suite services such as Fusion ERP and Oracle Fusion Cloud Enterprise Performance Management are deployed in separate identity domains, you can use SCIM provisioning to synchronize users and groups between them:

1. Create a confidential application in the source domain for SCIM provisioning. See Steps to Complete in the Source Identity Domain in IAM Interface.
2. Configure the GenericSCIM template in the target identity domain to establish connectivity with the source domain.
3. Initiate a full synchronization or set up a schedule for incremental updates in the target identity domain.

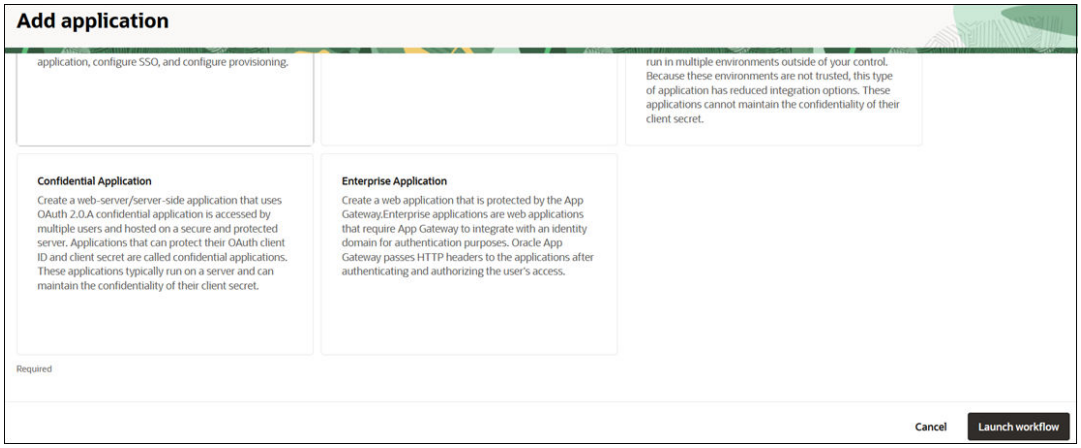
Steps to Complete in the Source Identity Domain in IAM Interface

Create and activate a confidential application in the source identity domain. Confidential applications run on a protected server and keep the OAuth client ID and client secret. The GenericSCIM application in the target identity domain uses these protected client credentials and connects with your source domain.

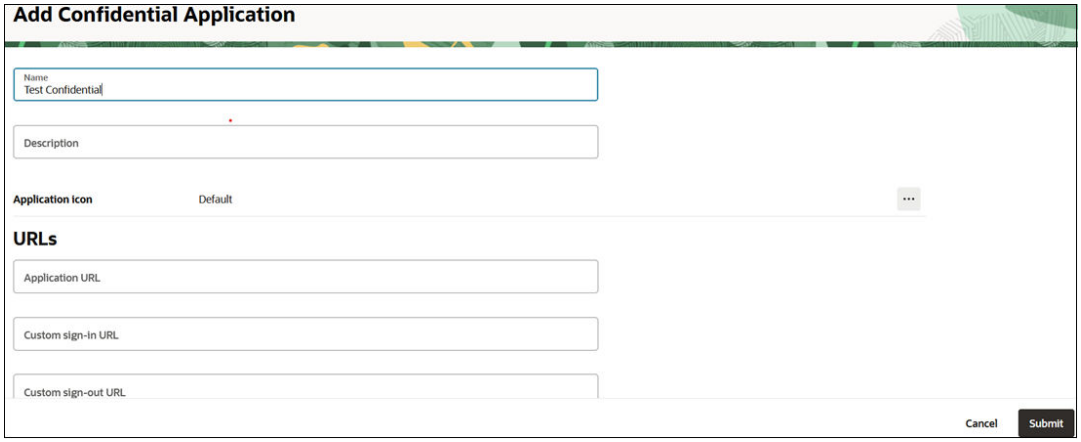
1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Select the domain to view the domains details page.
3. Navigate to the **Integrated applications** tab.



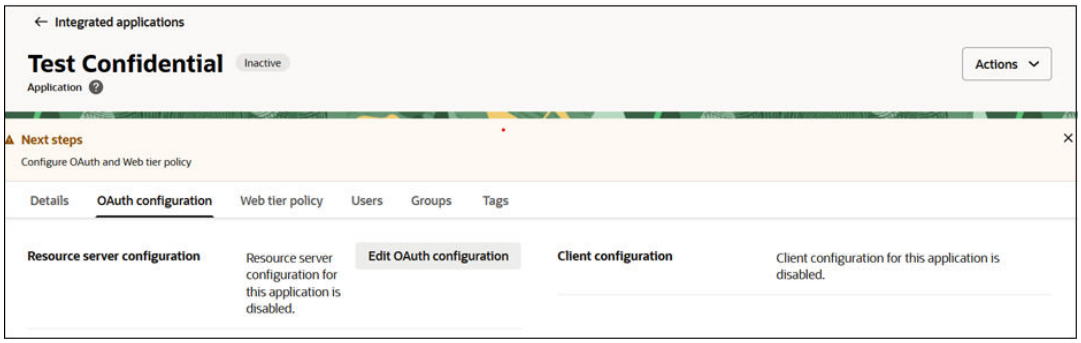
4. Click **Add application**.
5. On the **Add application** page, click **Confidential Application**, and then click **Launch workflow**.



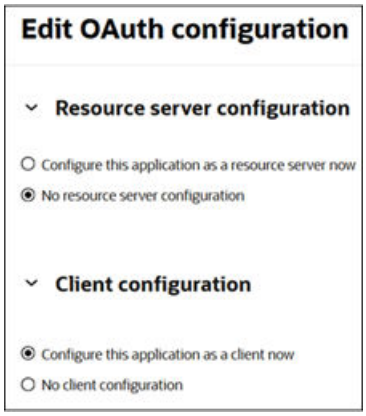
6. On **Add Confidential Application** page, enter the application name and other optional details.
7. Click **Submit** to create a new application.



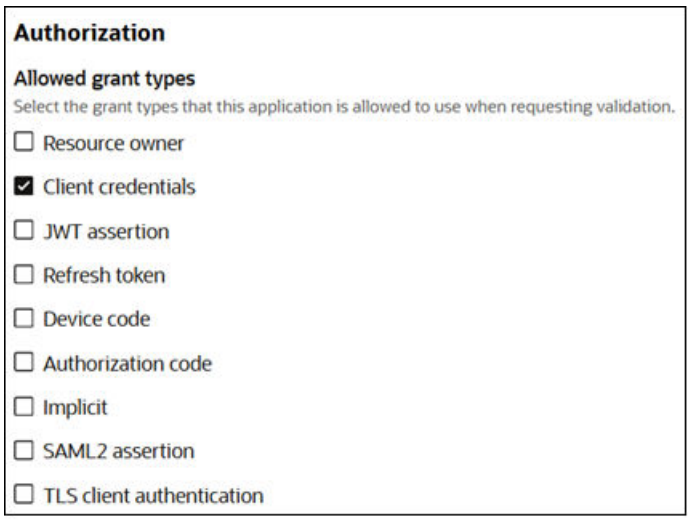
8. On the application's page, click **Oauth configuration** tab.



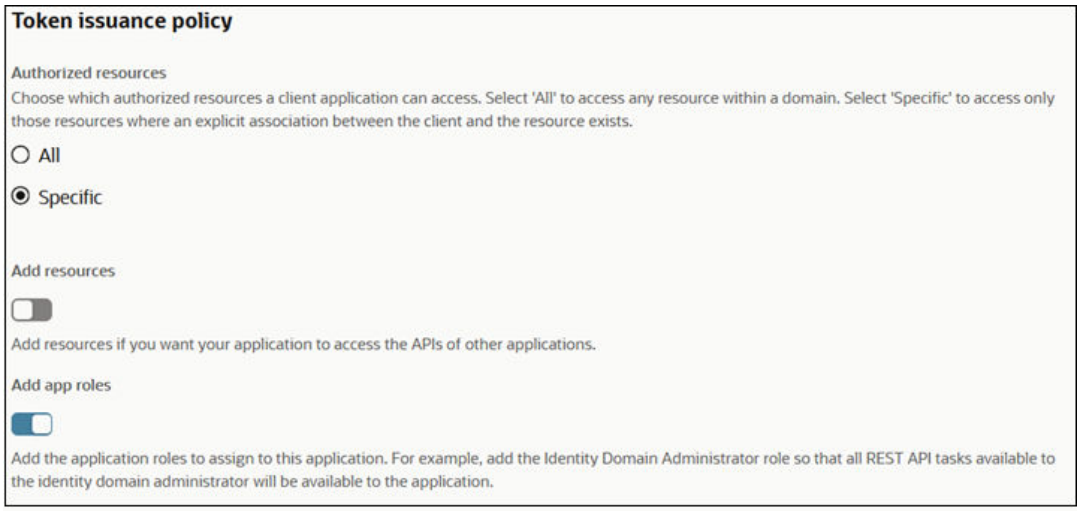
9. Click **Edit OAuth configuration**.
10. Select **Configure this application as a client now** for Client configuration.



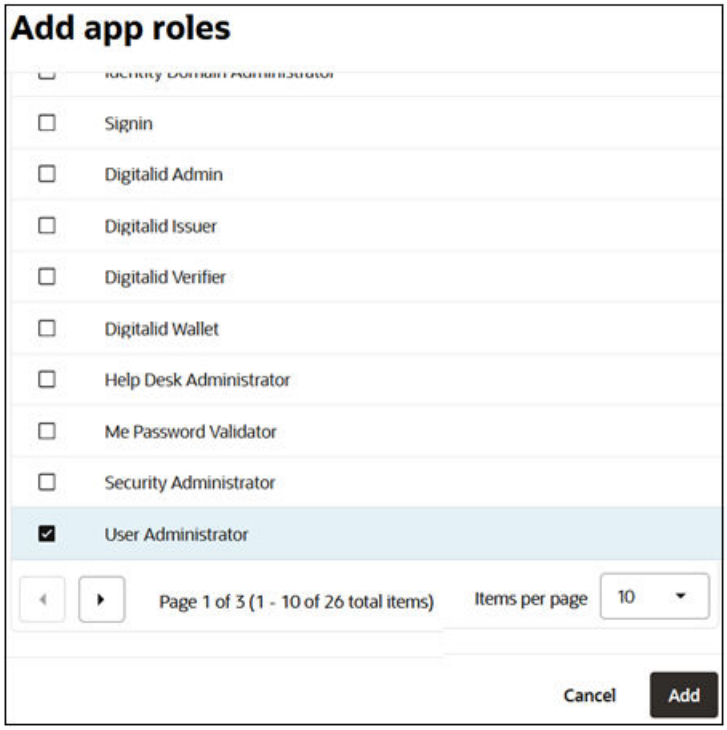
11. Select **Client Credentials** for **Authorization**.



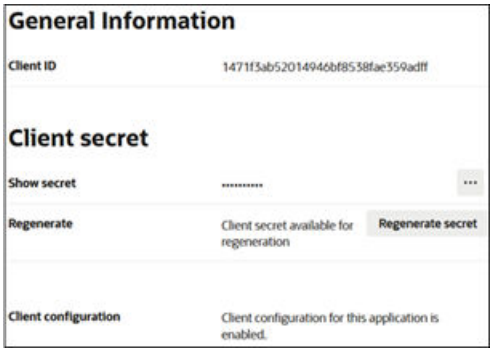
12. Scroll-down to the **Token Issuance Policy** section.
13. Click **Specific** for Authorized resources.
14. Click **Add app roles** and then click **Add app roles** again to proceed.



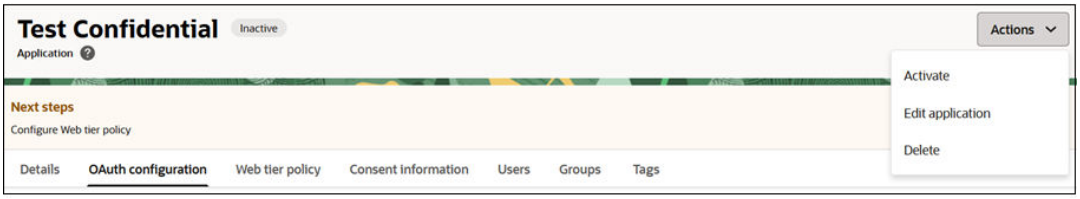
15. Select **User Administrator**, and click **Add**.



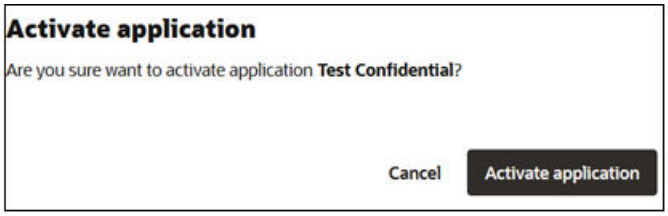
16. Click **Submit**.
17. In the General Information section, note the Client ID and Client Secret.



18. Click **Actions**, and select **Activate**.



19. On the confirmation page, click **Activate application** to finalize the activation.



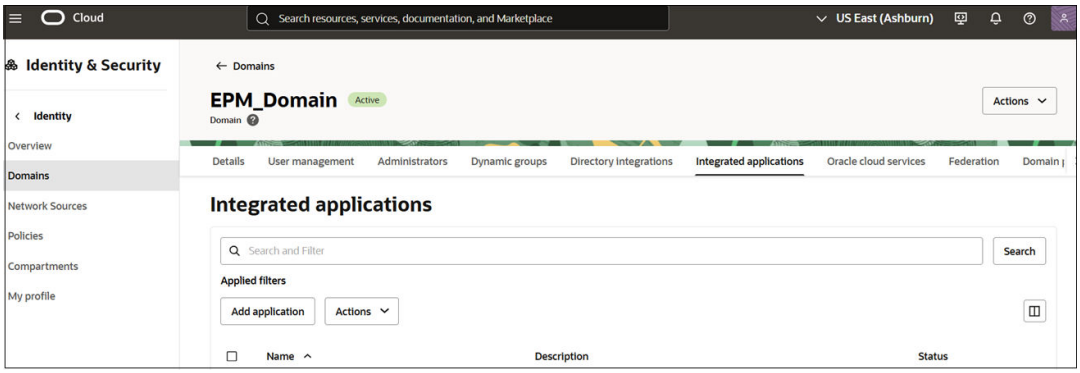
Steps to Complete in the Target Identity Domain in IAM Interface

Download Generic SCIM application template from the App Catalog of the target domain to enable and configure connectivity for synchronization.

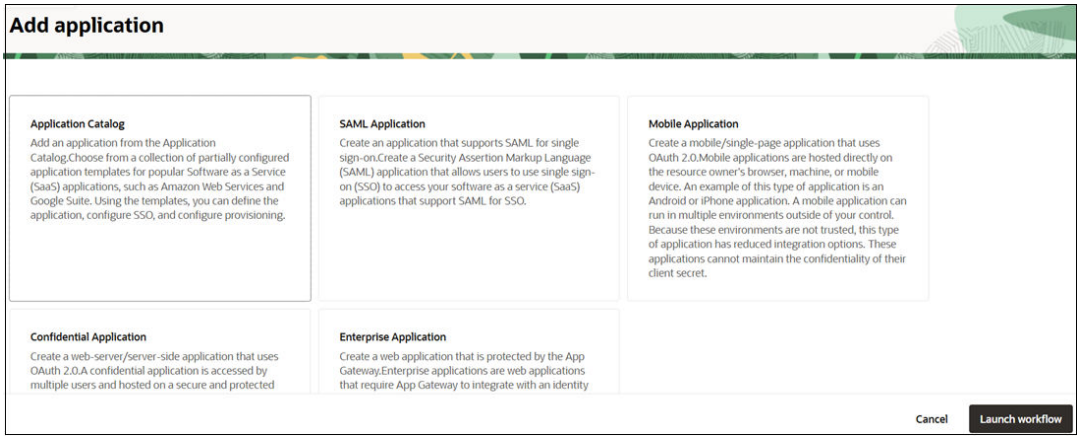
The Generic SCIM application template has been configured to enable Oracle Identity Cloud Service to communicate with applications that support SCIM. For more information, see How Do You Use the Generic SCIM App Template in Administering Oracle Identity Cloud Service?

Before you begin, note the Client ID and Client Secret of the application in the source identity domain. See Steps to Complete in the Source Identity Domain in IAM Interface

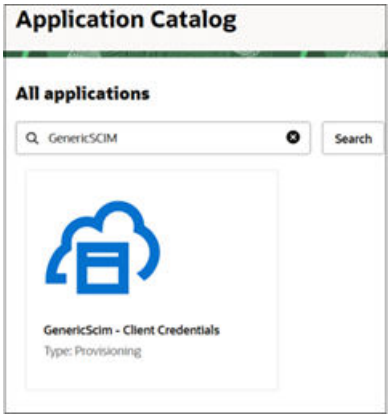
1. Sign into IAM Interface as an Identity Domain Administrator for the target domain. See Accessing the IAM Interface.
2. Select the domain to view the domains details page.
3. Navigate to the **Integrated applications** tab.



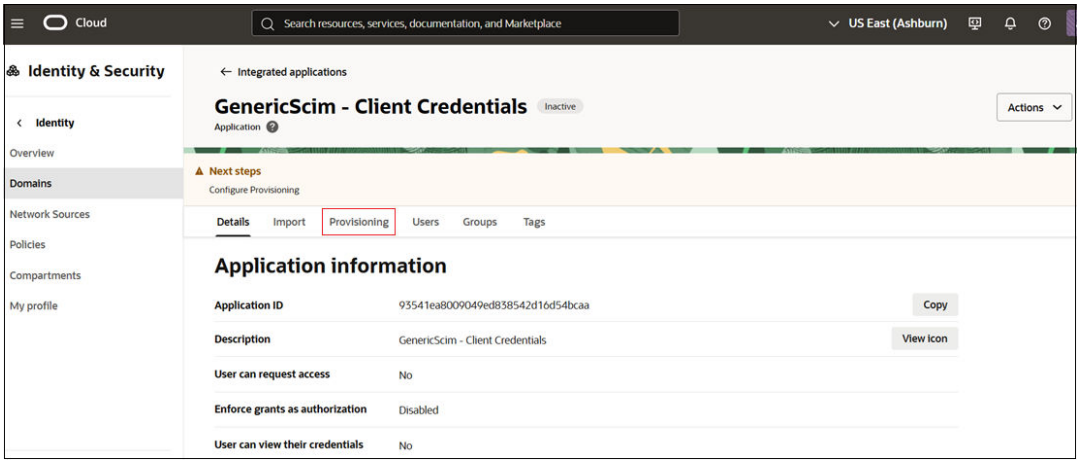
4. Click **Add application**.
5. On the **Add application** page, click **Application Catalog**, and then click **Launch workflow**.



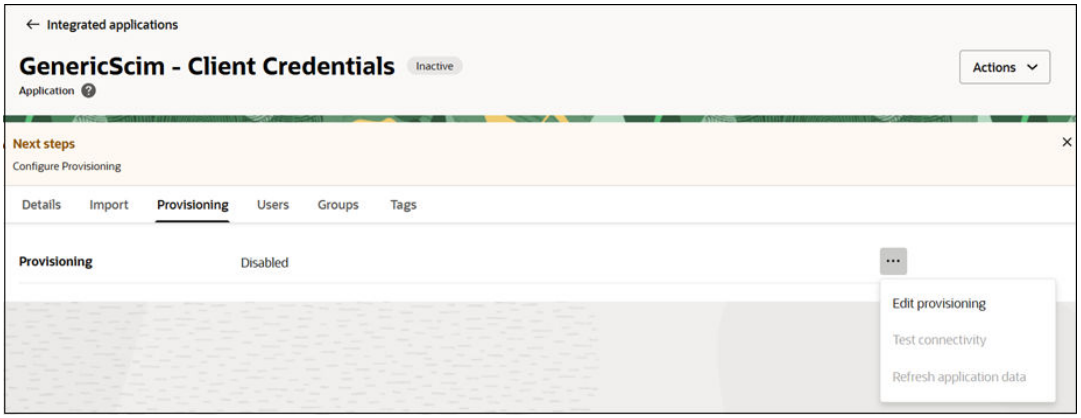
6. Search for *GenericSCIM* in App Catalog, and click **GenericScim - Client Credentials**.



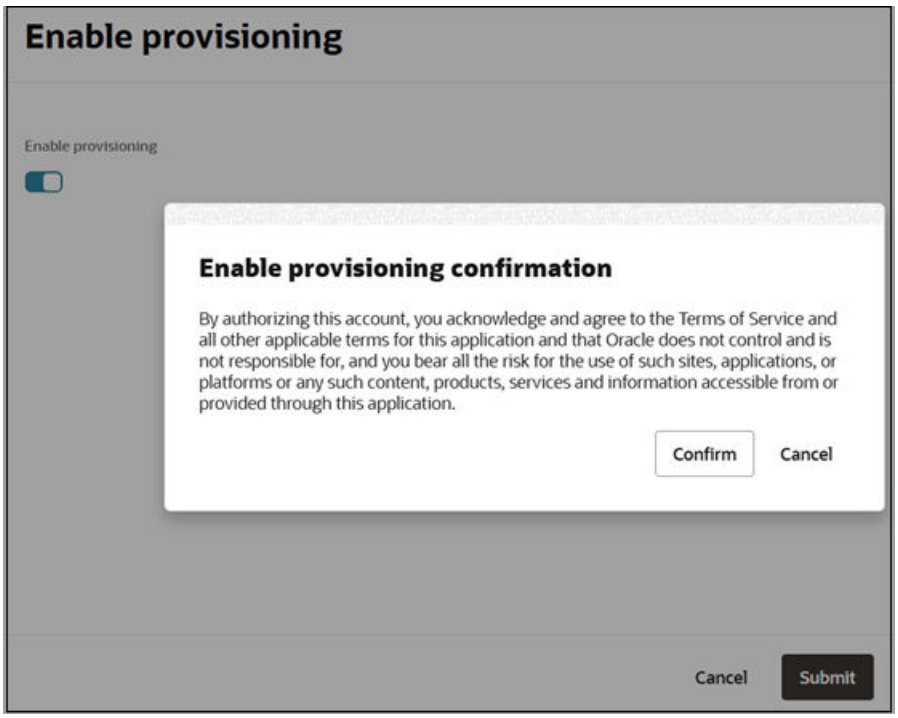
7. On the **Add GenericScim- Client Credentials** page, enter the required application details, and click **Submit**.
8. On the application page, navigate to the **Provisioning** tab.



9. Click **Ellipses (...)** button next to Provisioning header, and select **Edit provisioning**.



10. Click **Enable Provisioning**.
11. Click **Confirm** to close the confirmation message.

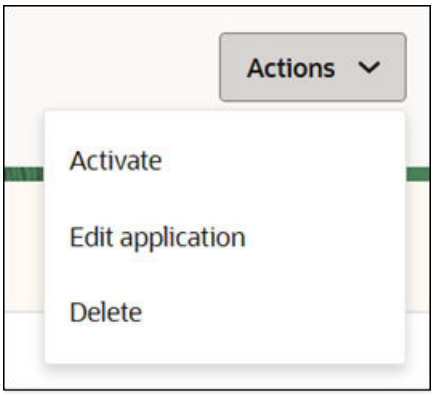


12. Under **Configure Connectivity**, enter the values for the following parameters:

Parameter	Description and Value Information
Host Name	If the SCIM interface's URL is `https://idcs.example.com/abc`, then the host name is `idcs.example.com`. This is the URL of the source identity domain.
Base URI	If the SCIM interface's URL is `https://idcs.example.com/admin/v1`, then the Base URI is `/admin/v1`.
Client Id	Client ID of the confidential application your created in the source identity domain.
Client Secret	Client Secret of the confidential application your created in the source identity domain.

Parameter	Description and Value Information
Scope	Use `urn:opc:idm:__myscopes__` as the scope of your application.
Authentication Server Url	The URL of your authentication server in the source domain. Example: `https://idcs.example.com/oauth2/v1/token`

13. Click **Test Connectivity** to verify the configuration.
14. Under **Select Provisioning Operations**, choose **Authoritative Sync**.
15. Select **Enable Synchronization**, then click **Submit**.
16. Back on the application page, click **Actions**, and select **Activate**.



17. On the confirmation dialog, click **Activate application**.

Synchronizing All Users and Groups in IAM Interface

To import users and groups, enable and configure synchronization for your application, and test your application to verify that users are provisioned correctly. See Synchronization Steps for All Users and Groups Using the IAM Interface

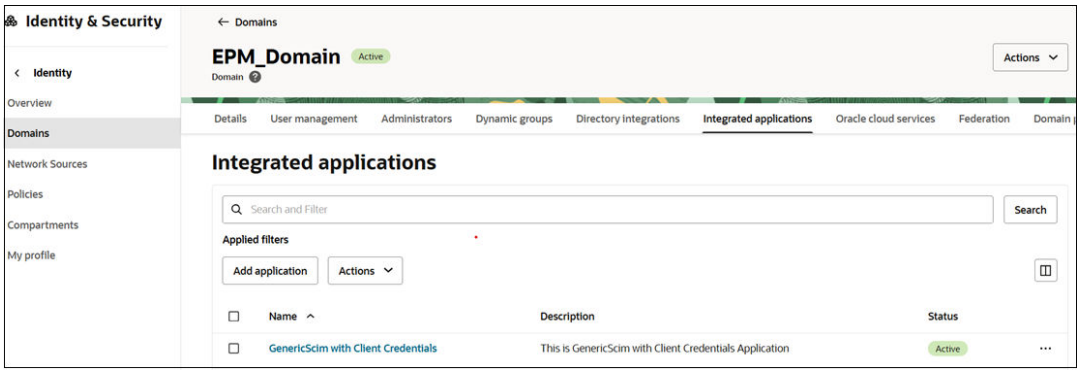
There are two methods to synchronize all users and groups:

- **Synchronize users and groups using Import** - Performs full synchronization to make sure that all changes made in the source identity domain are reflected in the target identity domain.
- **Schedule synchronization** - Makes incremental updates in the target domain:
  - Creates users and groups
  - Updates user and group details
  - Does not add or remove users from groups
  - Does not delete users or groups

Synchronize Users and Groups Using Import

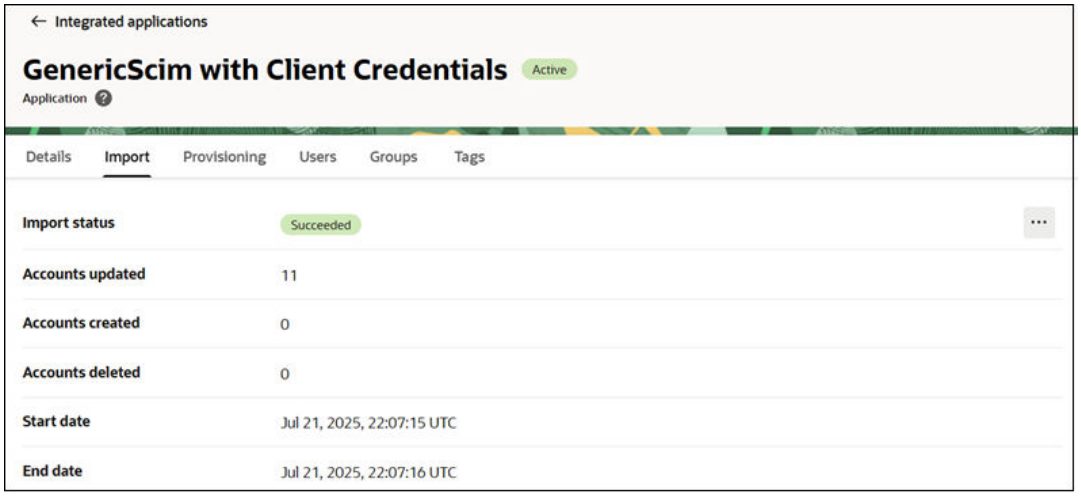
1. Sign into IAM Interface as an Identity Domain Administrator for the target domain. See: Accessing the IAM Interface.
2. Select the domain to view the domains details page.
3. Navigate to the **Integrated applications** tab.

4. Click **GenericScim - Client Credentials** application that you previously configured. See Steps to Complete in the Target Identity Domain in IAM Interface



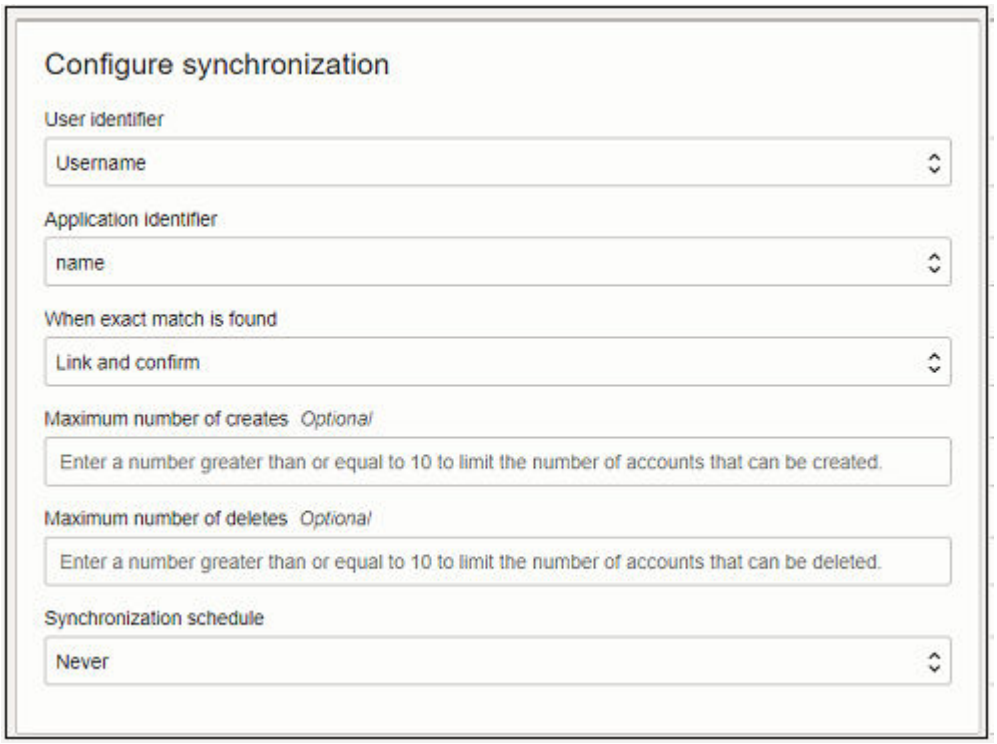
5. On the application page, go to the **Import** tab.
6. Next to **Import status**, click the **Ellipses ...** button, and select **Import**.
You see the message "`Your job for importing accounts is running`" until the job status changes to "Succeeded".

   All the users and groups from the source environment will get imported, and the **Synchronization Status** of each user will display **Confirmed**.



Schedule Synchronization

1. On the same application page, navigate to the **Provisioning** tab.
2. Click **Edit Provisioning**, and scroll to the **Configure Synchronization** section.
3. Choose the appropriate option for **Synchronization schedule**.



4. Click **Submit** to save and apply the schedule.

Synchronization Steps for Specific Users and Groups in IAM Interface

Follow the step-by-step instructions in the links provided to synchronize specific users and groups from a source domain to a target domain (within the same cloud account or across separate cloud accounts):

1. Create a confidential application in the target identity domain. If needed, create a new group in the target domain so that you can assign users in the source domain to this group once the source and target domains are integrated. See Steps to Complete in the Target Identity Domain in IAM Interface.
2. Create and configure connectivity settings in the Oracle Identity domain application in the source identity domain. See Steps to Complete in the Source Identity Domain in IAM Interface.
3. Perform synchronization of specific users and groups in the source domain. See Synchronizing Specific Users and Groups in IAM Interface.

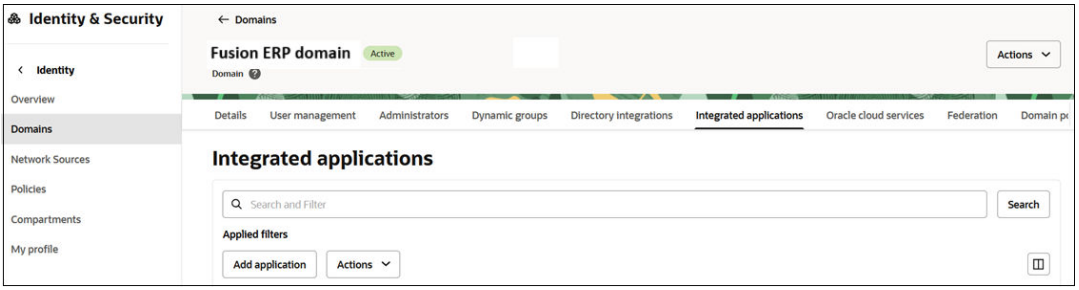
Steps to Complete in the Target Identity Domain in IAM Interface

Create and activate a confidential application in the target identity domain. Confidential applications run on a protected server and keep the OAuth client ID and client secret. The Oracle Identity Domain application in the source identity domain uses these protected client credentials and connects with your target domain. See Create and Activate a Confidential Application.

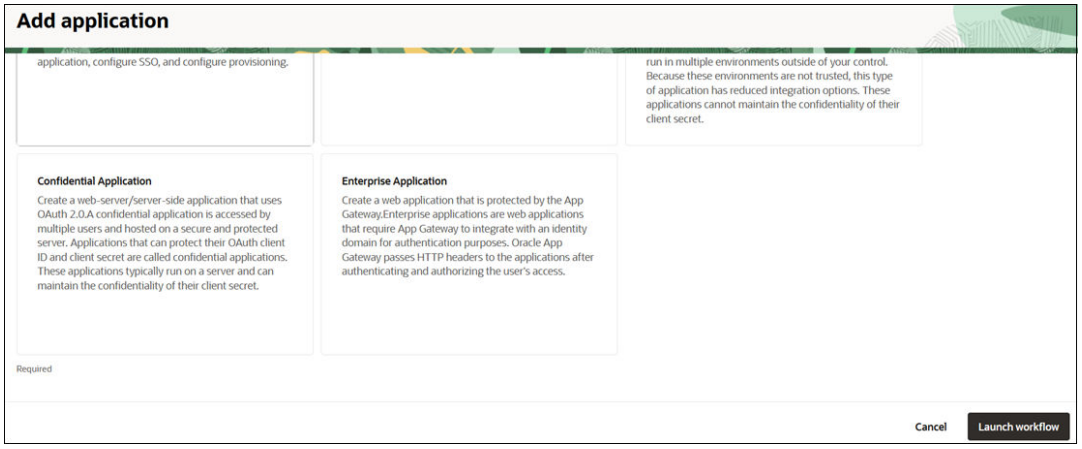
If needed, create a new group in the target domain so that you can assign users in the source domain to this group once the source and target domains are integrated. See Creating IDCS Groups.

Create and Activate a Confidential Application

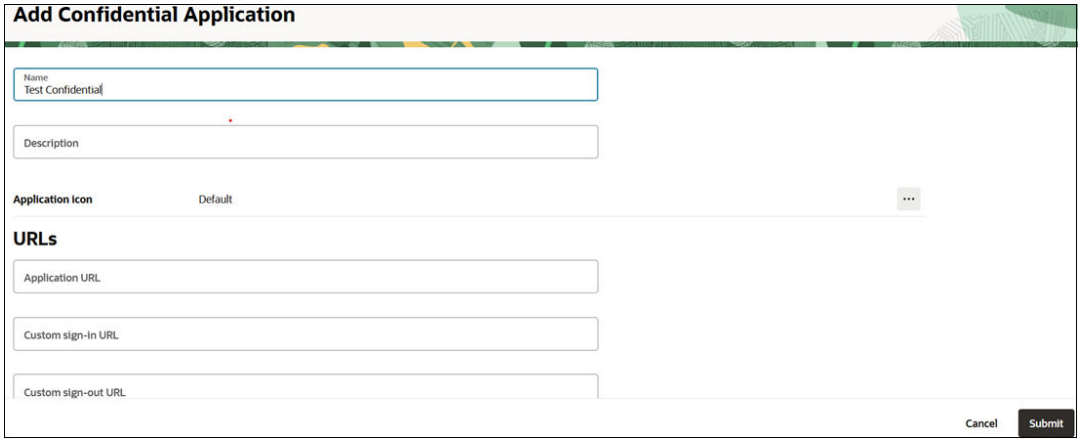
1. Sign into IAM Interface as an Identity Domain Administrator in the target domain. See Accessing the IAM Interface.
2. Navigate to the **Integrated applications** tab.



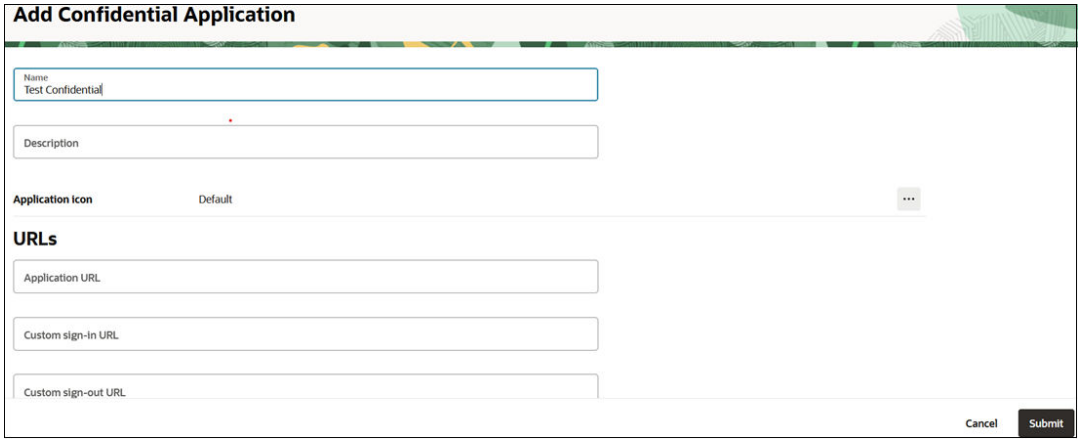
3. Click **Add application**.
4. On the **Add application** page, click **Confidential Application**, and then click **Launch workflow**.



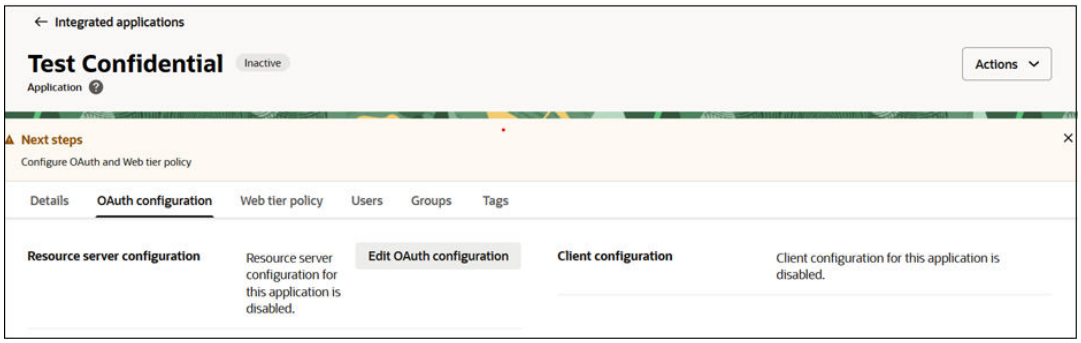
5. Click **Submit** to create a new application.



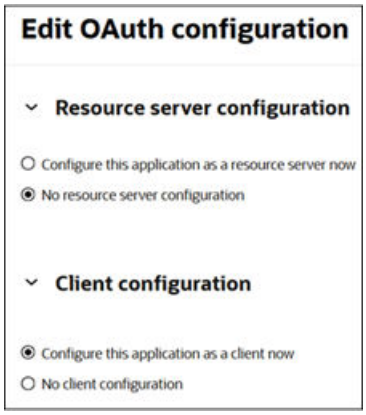
6. Click **Submit** to create a new application.



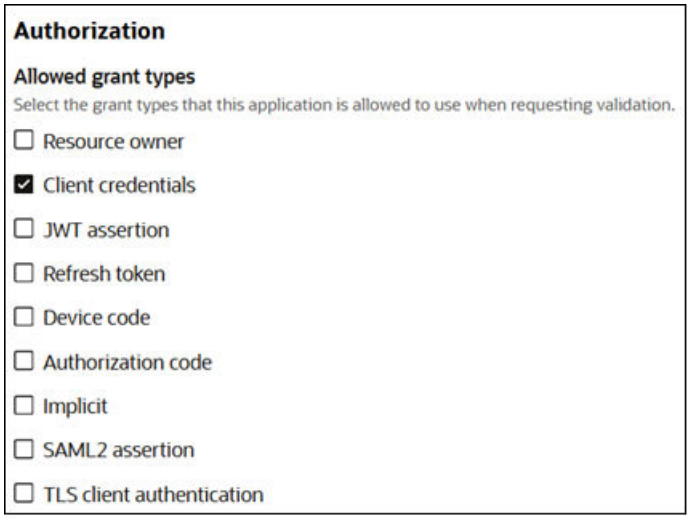
7. On the application's page, click **Oauth configuration** tab.



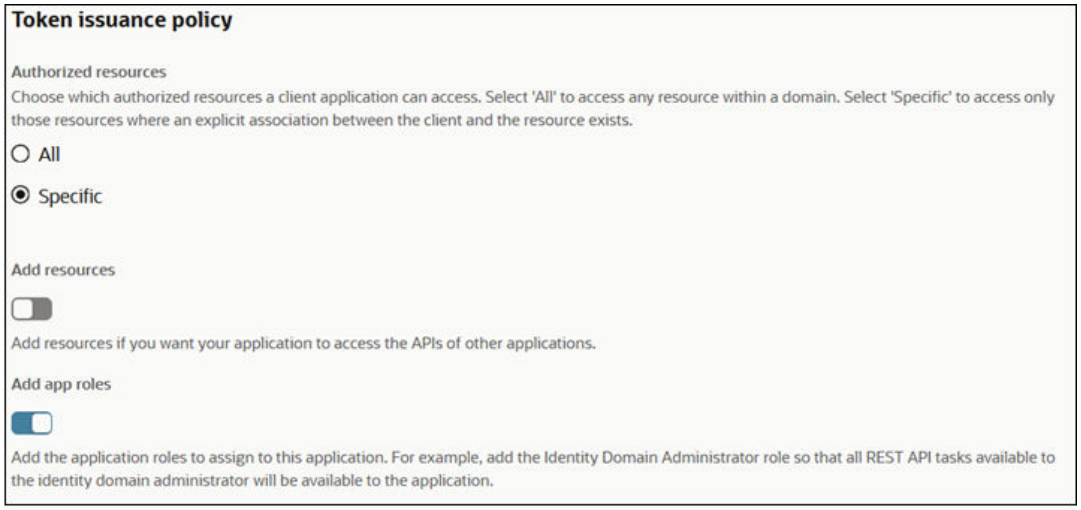
8. Click **Edit OAuth configuration**.
9. Select **Configure this application as a client now** for Client configuration.



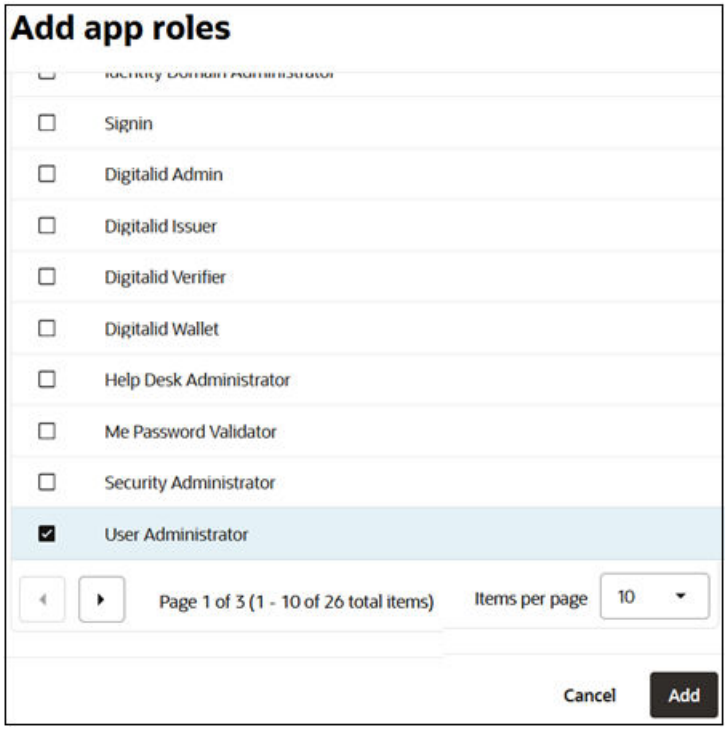
10. Select **Client Credentials** for **Authorization**.



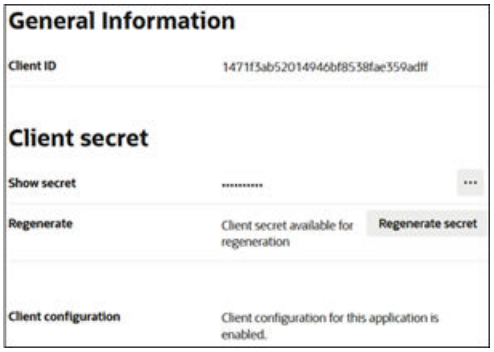
11. Scroll-down to the **Token Issuance Policy** section.
12. Click **Specific** for Authorized resources.
13. Click **Add app roles** and then click **Add app roles** again to proceed.



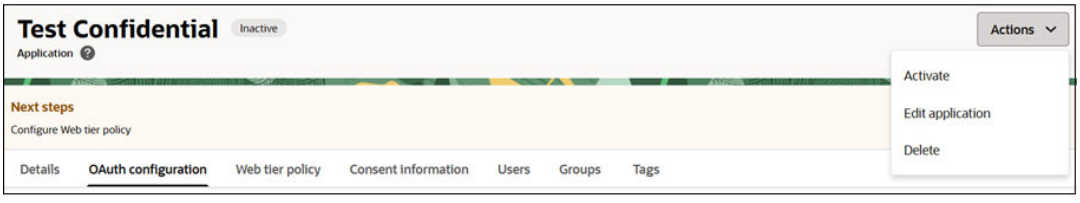
14. Select **User Administrator**, and click **Add**.



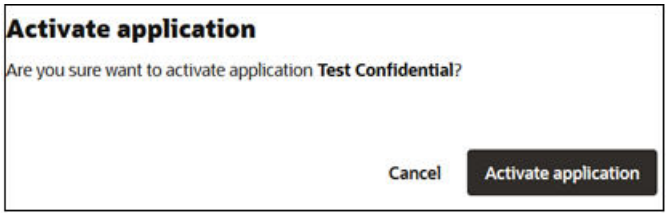
15. Click **Submit**.
16. In the General Information section, note the Client ID and Client Secret.



17. Click **Actions**, and select **Activate**.



18. On the confirmation page, click **Activate application** to finalize the activation.

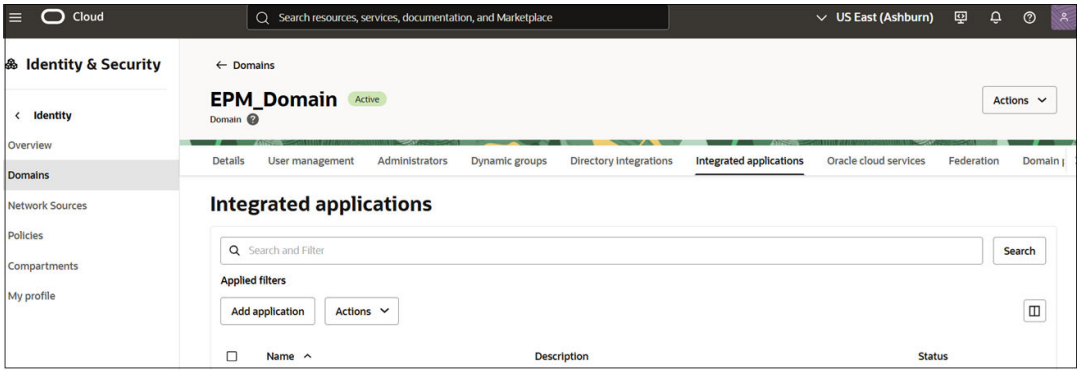


Steps to Complete in the Source Identity Domain in IAM Interface

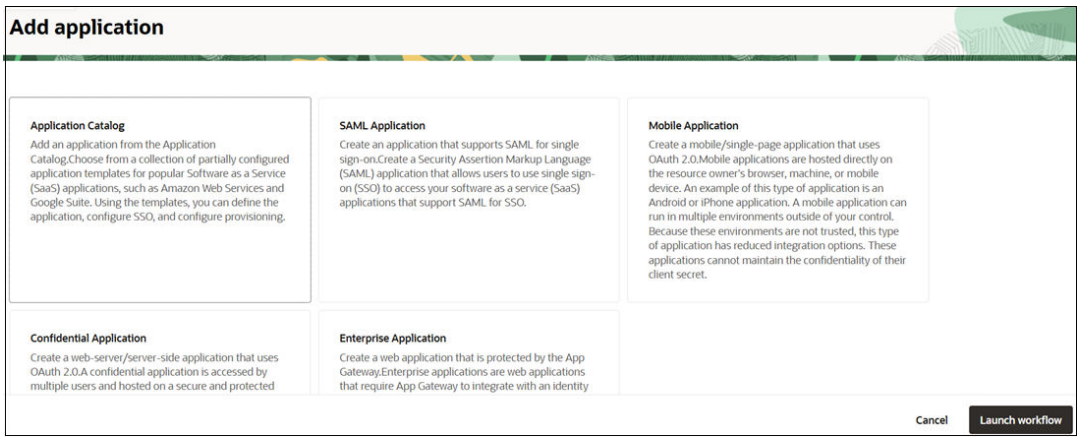
Download Oracle Identity Domain application from the App Catalog of the target domain to enable and configure connectivity for synchronization.

Before you begin, note the Client ID and Client Secret in **General Information** of the application in the target identity domain. See Steps to Complete in the Target Identity Domain in IAM Interface

1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Navigate to the **Integrated applications** tab.

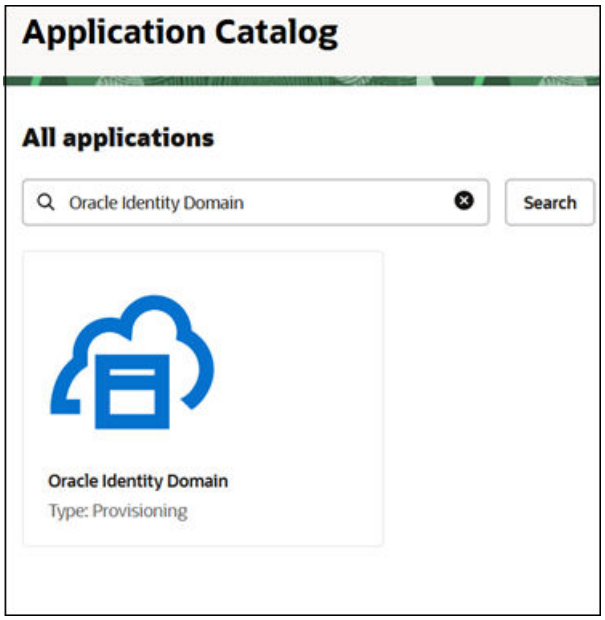


3. Click **Add application**.
4. On the **Add application** page, click **Application Catalog**, and then click **Launch workflow**.



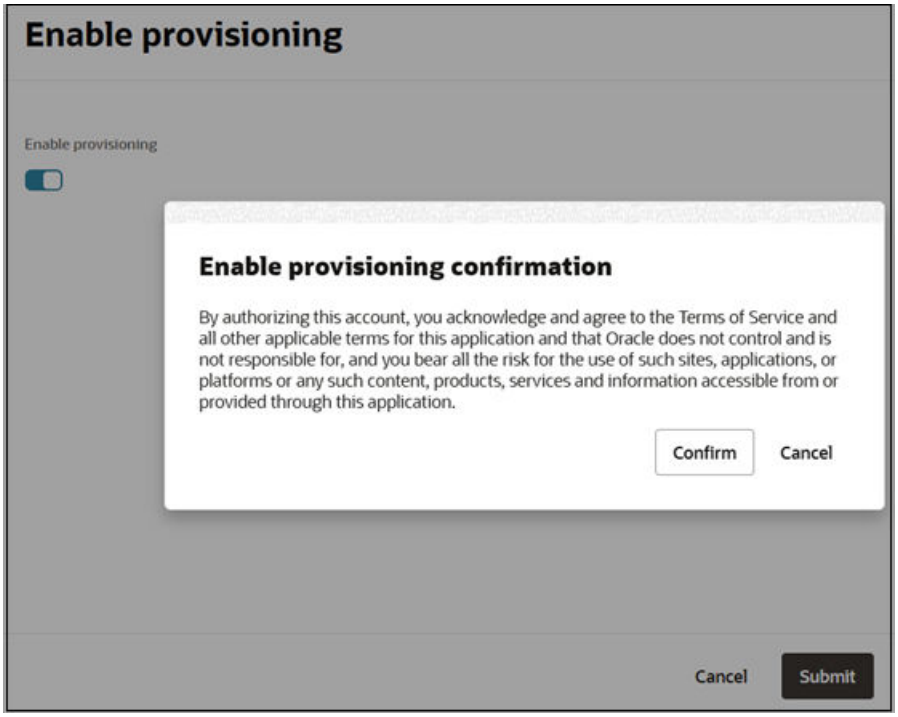
5. Search for *Oracle Identity Domain* in App Catalog, and click **Oracle Identity Domain**.

6. Search for *Oracle Identity Domain* in App Catalog, and click **Add** next to **Oracle Identity Domain**.



7. On the **Add Oracle Identity Domain** page, enter the required application details, and click **Submit**.
8. On the application page, navigate to the **Provisioning** tab.

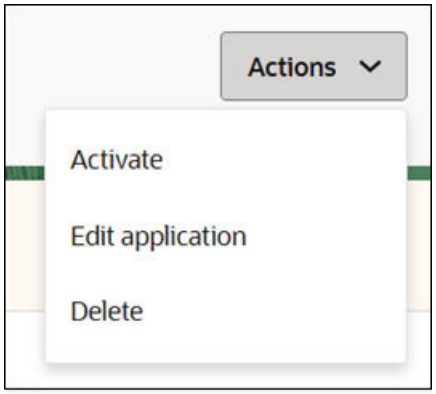
9. Click **Ellipses (…)** button next to Provisioning header, and select **Edit provisioning**.
10. Click **Enable Provisioning**.
11. Click **Confirm** to close the confirmation message.



12. In **Configure Connectivity**, enter the values for the following parameters:

Parameter	Description and Value Information
Host Name	If the SCIM interface's URL is `https://idcs.example.com/abc`, then the host name is `idcs.example.com`. This is the URL of the target identity domain.
Client Id	Client ID of the confidential application your created in the target identity domain.
Client Secret	Client Secret of the confidential application your created in the target identity domain.
Scope	Use `urn:opc:idm:__myscopes__` as the scope of your application.
Authentication Server Url	The URL of your authentication server in the target domain. Example: `https://idcs.example.com/oauth2/v1/token`

13. Click **Test Connectivity** to verify the configuration.
14. Under **Select Provisioning Operations**, choose **Authoritative Sync**.
15. Select **Enable Synchronization**, then click **Submit**.
16. Back on the application page, click **Actions**, and select **Activate**.



17. On the confirmation dialog, click **Activate application**.

Synchronizing Specific Users and Groups in IAM Interface

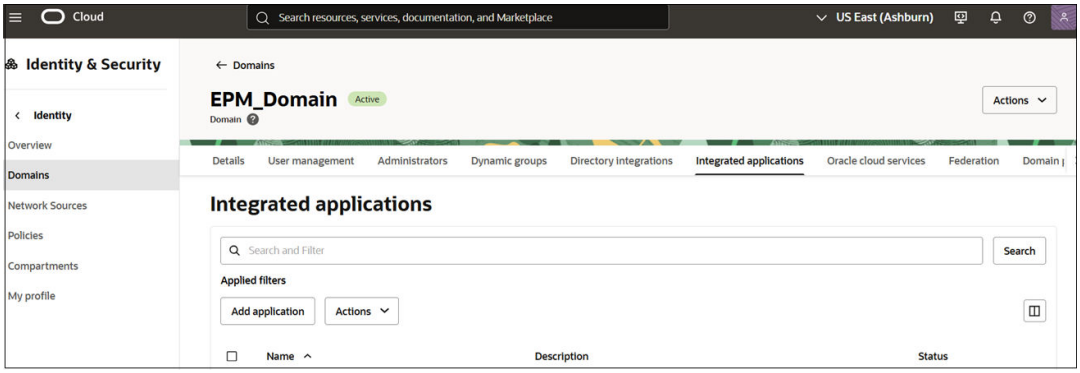
To provision specific users and groups, enable and configure synchronization for your application, and test your application to verify that users are provisioned correctly. See Synchronization Steps for Specific Users and Groups in IAM Interface

There are three methods to synchronize specific users and groups. You can:

- Synchronize users without any group membership
- Synchronize users with membership to a specific group in the target domain
- Synchronize a group in the source domain to a specific group in the target domain

Synchronize Users Without Any Group Membership

1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Navigate to the **Integrated applications** tab.

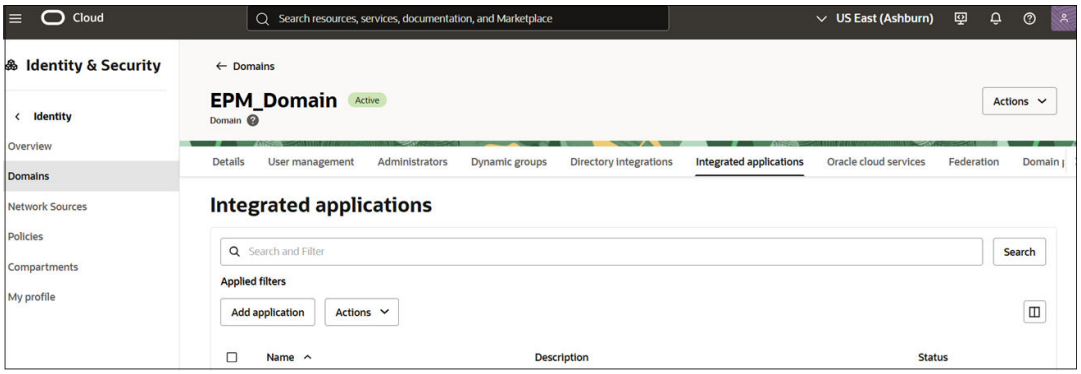


3. Click on the Oracle Identity Domain application that you created earlier. See Steps to Complete in the Source Identity Domain in IAM Interface
4. Navigate to the **Users** tab.
5. Click **Assign users**.
6. On **Assign Users** page, search and select the user, and then click **Assign**.
The user will now be provisioned in the target domain.

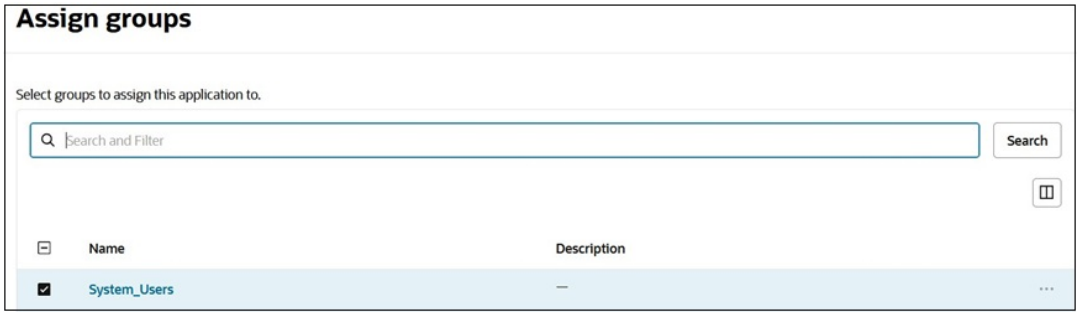
Synchronize Users with Membership to a Specific Group in the Target Domain

Identify the group to which you want to map the required users in the target domain. If needed, create an Identity Cloud Service group. See Creating IDCS Groups.

1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Navigate to the **Integrated applications** tab.

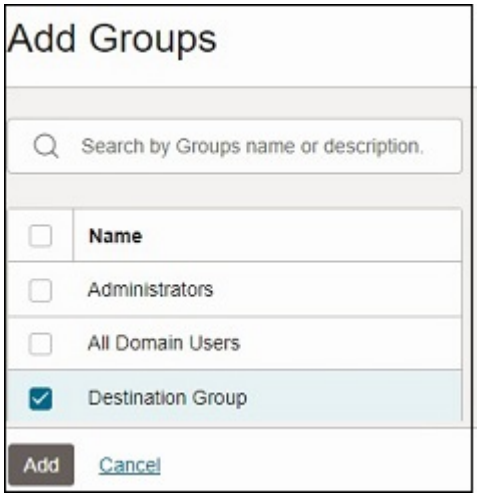


3. Click on the Oracle Identity Domain application that you created earlier. See Steps to Complete in the Source Identity Domain in IAM Interface
4. Navigate to **Provisioning** tab.
5. Click **ellipses** next to Provisioning, and select **Refresh Application Data**.
6. Click **Provisioning** under **Resources**, and then click **Refresh Application Data**.
7. Navigate to **Groups** tab.
8. Click **Assign groups**.
9. On Assign groups page, search and select the groups, and then click **Assign**
   The group will now get access to the application.



10. Click the group name that you want to assign certain users.
11. Navigate to the **Users** tab.
12. Click **Assign user to group**.
13. On **Assign Users** page, search and select the user, and then click **Assign**.
    The user will now assigned access to the application.

14. On **Add Groups**, search and select the group in the target domain to assign to this user.



15. Click **Add**, and then click **Assign user**.
    The user will now be provisioned to the group in the target domain.

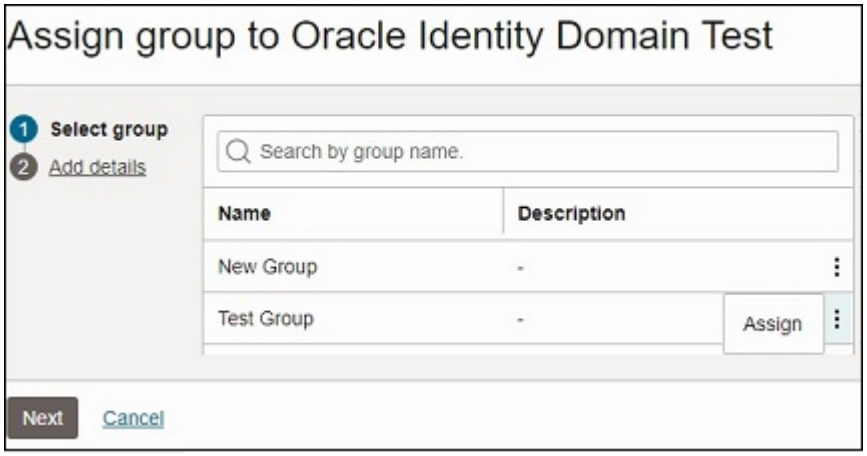
Synchronize a Group at Source Domain to a Specific Group in the Target Domain

Identify a group in the source domain and one in the target domain. If needed, create an Identity Cloud Service group.

1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Click **Applications** under **Identity domain**.
3. Click on the Oracle Identity Domain application that you created earlier. See Steps to Complete in the Source Identity Domain in IAM Interface
4. Click **Provisioning** under **Resources**, and then click **Refresh Application Data**.

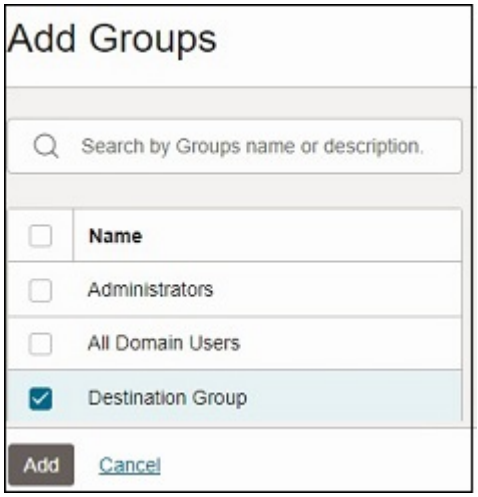
5. Click **Groups** under **Resources**, and then click **Assign groups**.

6. On **Assign group to application** page, search and select the group, and then click **Assign** on the menu next to the group.



7. Click **Next**.
8. On **Add details**, scroll down and check **Groups**, and then click **Add**.

9. On **Add Groups**, search and select the group in the target domain to assign to this user.



10. Click **Add** and then click **Assign group**.
Users in the source group will now be provisioned in the selected group in the target domain.

Synchronizing Users and Groups from Microsoft Entra ID to IAM

Using SCIM, Identity Domain Administrators can smoothly integrate Microsoft Entra ID with IAM, enabling automatic synchronization of users and groups between the two systems. This section outlines the steps:

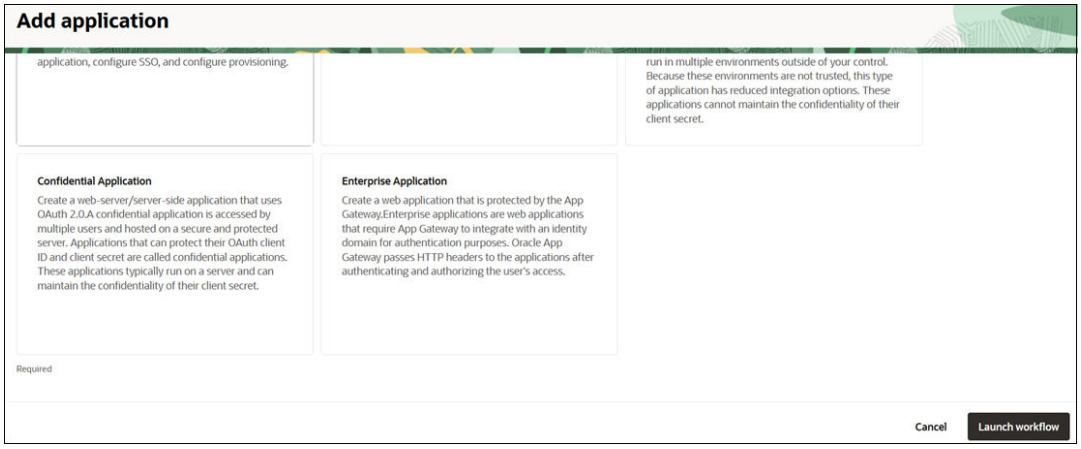
- Step 1: Setting Up SSO with Cloud EPM Using Microsoft Entra ID
- Step 2: Creating a Confidential Application to Configure Authorization
- Step 3: Configuring Connectivity for Synchronization with Microsoft Entra ID

Step 1: Setting Up SSO with Cloud EPM Using Microsoft Entra ID

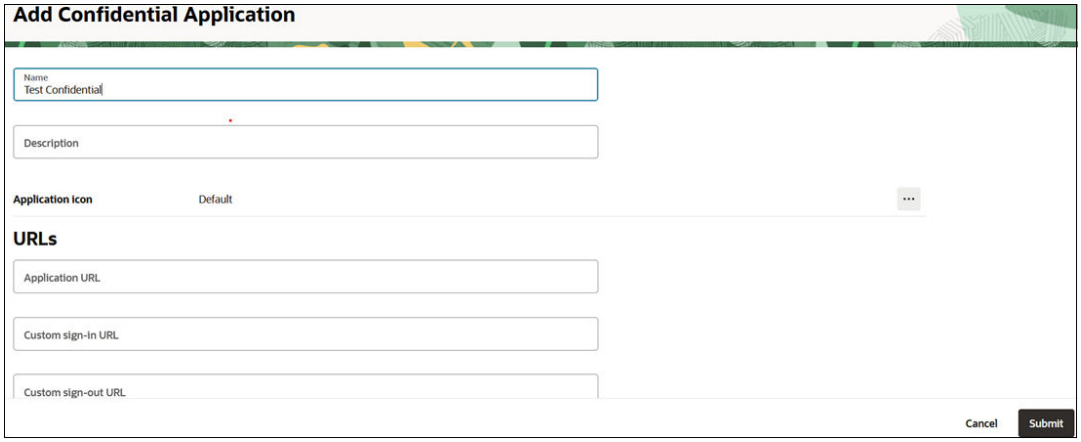
1. Add IAM as an enterprise application in Microsoft Entra ID. See Steps to Complete in Microsoft Entra ID.
2. Set up Microsoft Entra ID as the IdP in the IAM Interface. See Steps to Complete in Oracle Cloud Console.

Step 2: Creating a Confidential Application to Configure Authorization

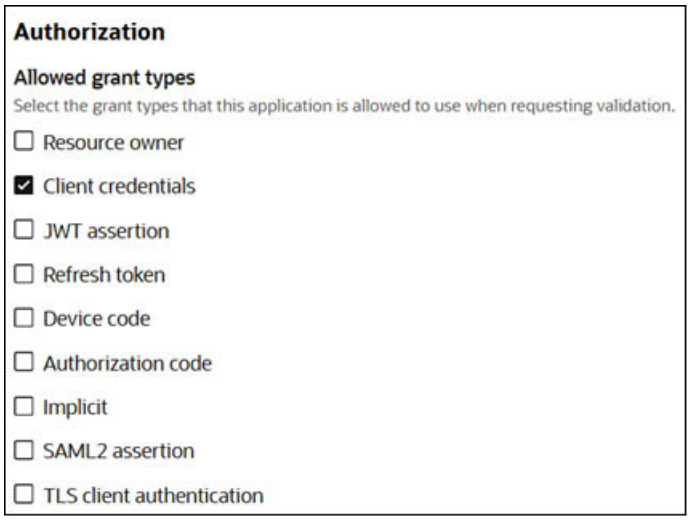
1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Click **Integrated applications** under **Identity domain**.
3. Click **Add application**.
4. On the **Add application** page, select **Confidential Application**, and then click **Launch workflow**.



5. On **Add application details**, enter application name and other optional details, and then click **Next**.

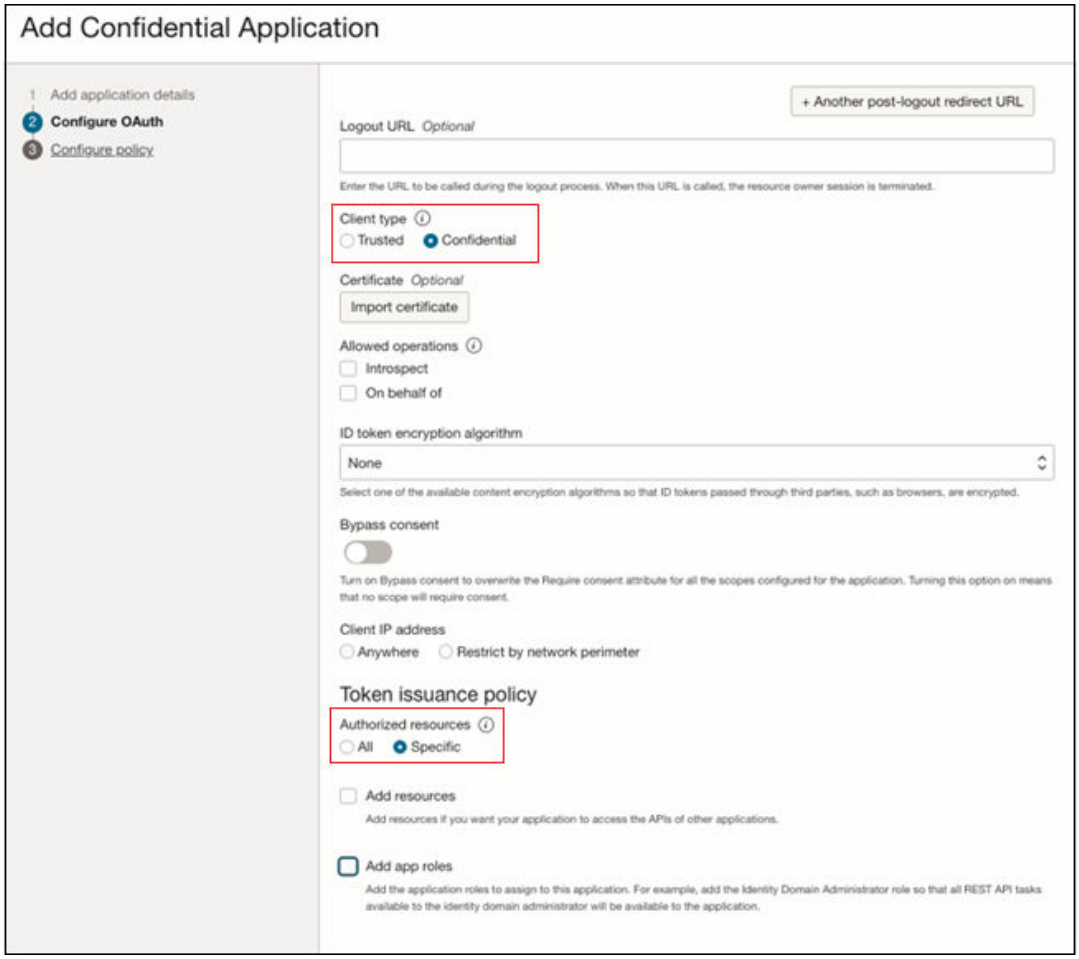


6. On **Configure OAuth**, select **Configure this application as a client now**.
7. Select **Client Credentials** for **Authorization**.

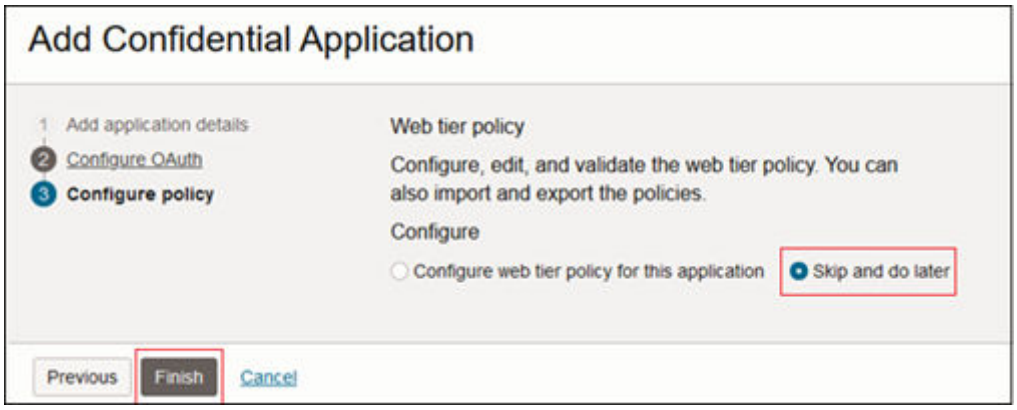


8. Select **Confidential** for **Client type**.

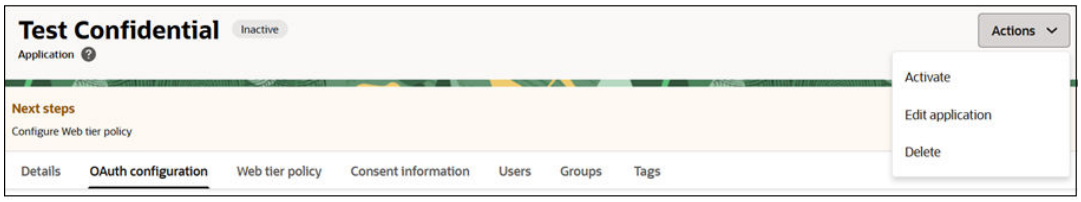
9. Scroll-down to **Token Issuance Policy**, and click **Specific** for **Authorized resources**.



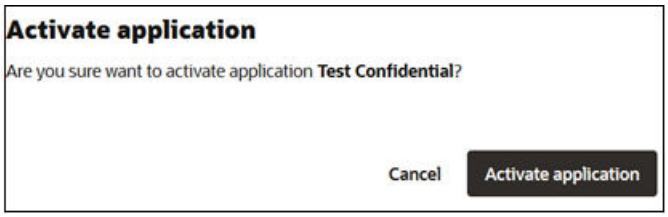
10. Click **Next**.
11. For **Configure policy**, keep the default setting **Skip and do later**, and then click **Finish**. The application is added



12. Click **Activate**.

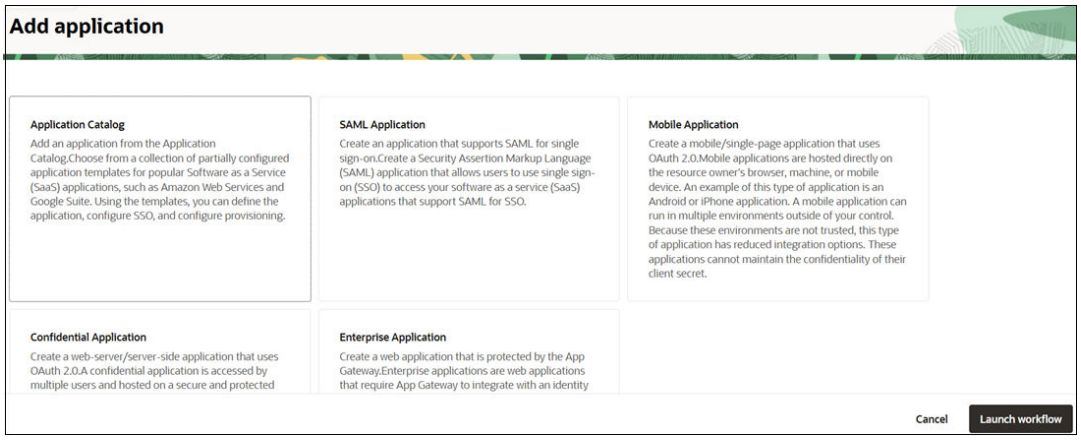


13. On the **Activate Application** page, click **Activate application** to confirm activation.

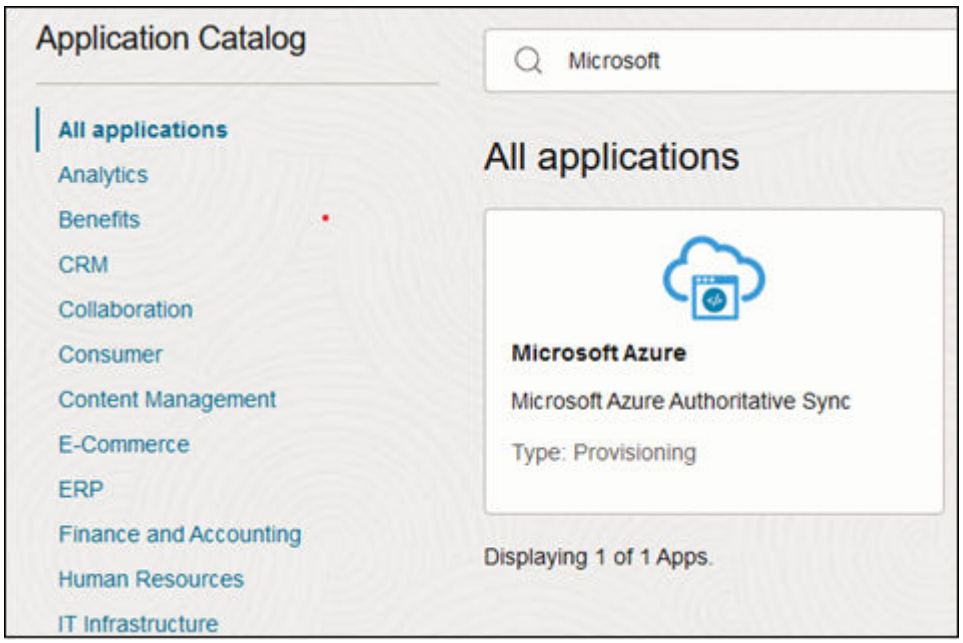


Step 3: Configuring Connectivity for Synchronization with Microsoft Entra ID

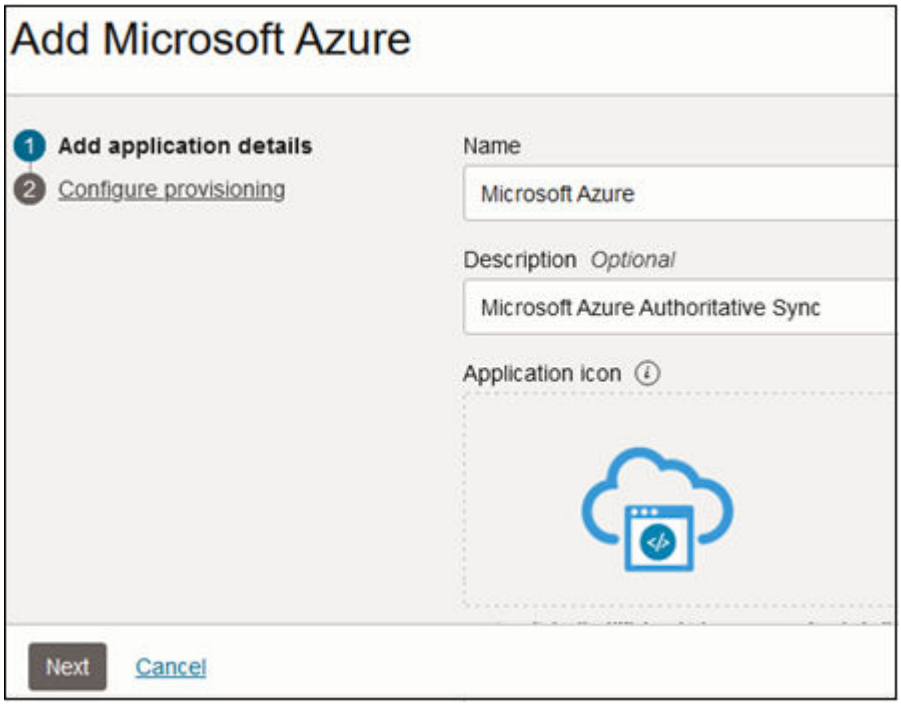
1. Click **Integrated applications** under **Identity domain**.
2. Click **Application Catalog**, and then click **Launch app catalog**.



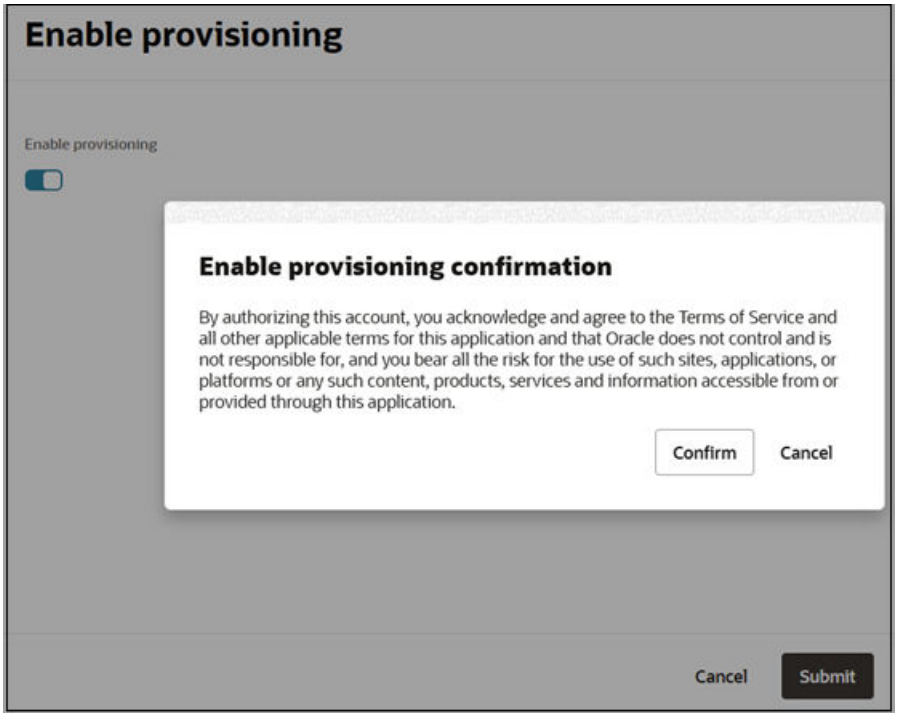
3. Search for *Microsoft* in the App Catalog, and click **Add** next to **Oracle Identity Domain**.



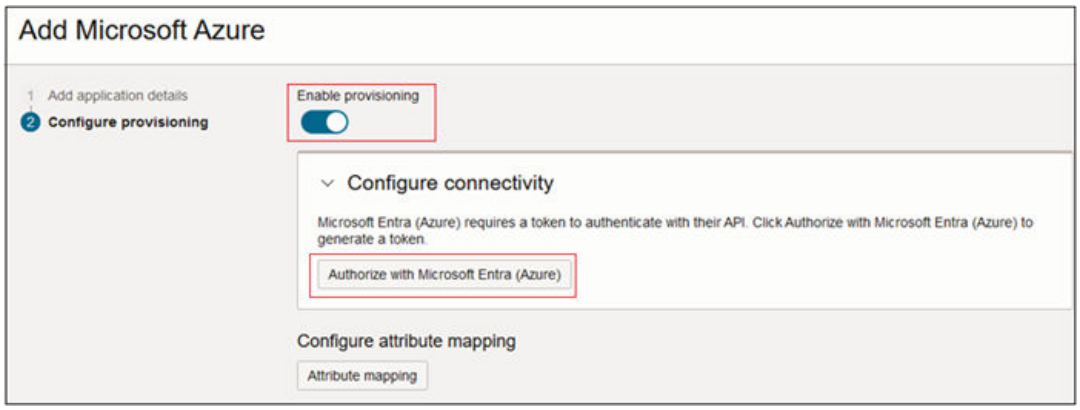
4. Add application details, and click **Next**.



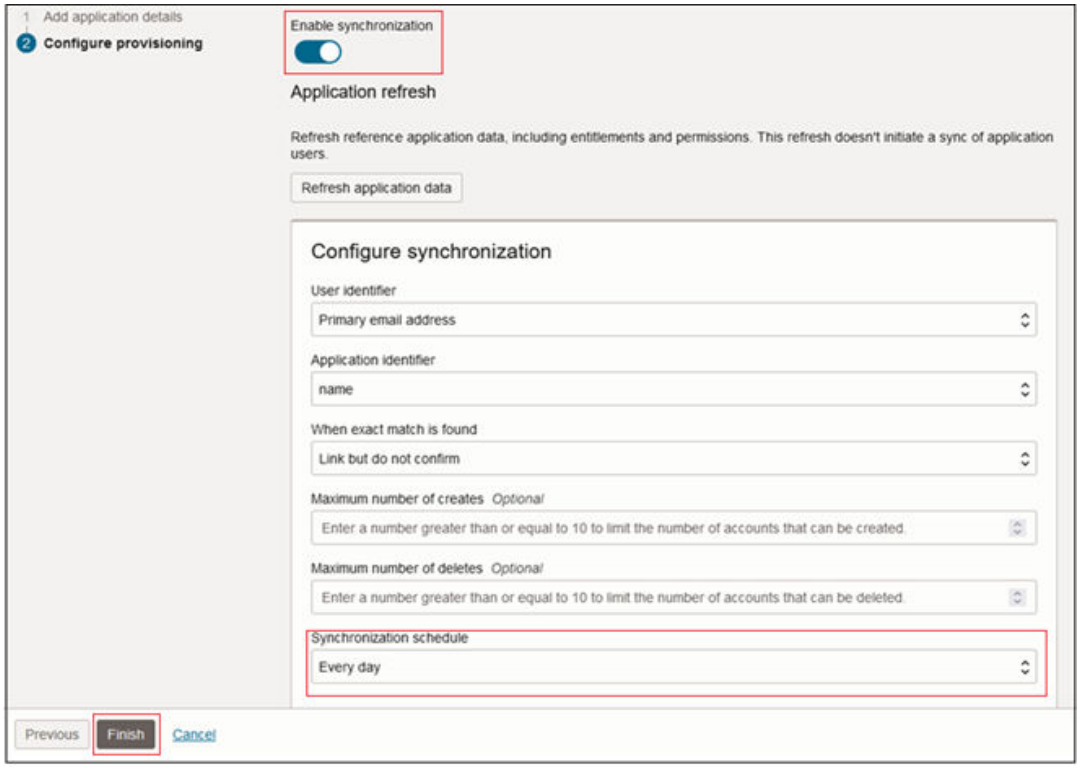
5. Click **Enable Provisioning**. and then click **Confirm** to close the confirmation message.



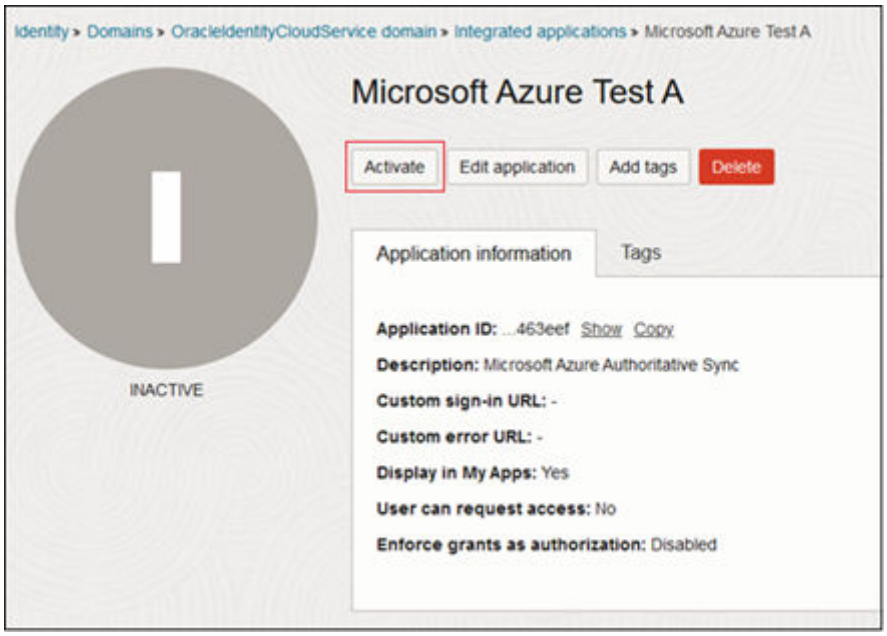
6. Under **Configure Connectivity**, click **Authorize with `Microsoft Entra ID Application Name`**.



7. After authorizing Microsoft Entra ID, scroll-down and click **Enable synchronization**.
8. Under **Configure synchronization**, select **Synchronization schedule**.
9. Click **Finish**.



10. On the application page, click **Activate** to activate the Microsoft Entra ID application. Users and groups will sync automatically between Microsoft Entra ID and IAM based on the configured schedule.



Creating Groups for Application-Level Role Assignment

The following applications (business processes) allow you to create groups. You can assign identity domain users or other groups as children of a group.

- Planning
- Planning Modules
- FreeForm
- Financial Consolidation and Close
- Enterprise Profitability and Cost Management
- Tax Reporting

Group information is maintained independently by each Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environment. For information on creating groups and assigning application-level roles, see *Administering Access Control*.

Email Notifications

By default, the Cloud Account Administrator (`oraclecloudadmin_ww@epm.oraclecloud.com`) sends an email to each new user.

The email contains the credentials (user name and a temporary password) that the user needs to sign in to the environment.

- User names must contain only ASCII characters and must be unique within the identity domain.
- If used as the user name, the email ID must be unique.
- The first name, last name and email ID of users may contain the apostrophe punctuation mark (').
- Email IDs containing the apostrophe punctuation mark cannot be used as the user name. Use these information sources:

If the users are added through Oracle Cloud Console, EPM Automate, or REST API, the emails are sent as they are added.

> **Note**
>
> You can modify the notification templates for the email notifications from Identity Cloud Service 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. For detailed information, see Customize Oracle Identity Cloud Service Notifications in *Administering Oracle Identity Cloud Service*.

How to Avoid Welcome Email Notifications for Newly Created Users

When you configure Single Sign On (SSO) with an identity provider (IdP), import user information from a file into IAM Interface to prevent Welcome Email Notifications to be sent to users. The import file should have the following fields:

```
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
```

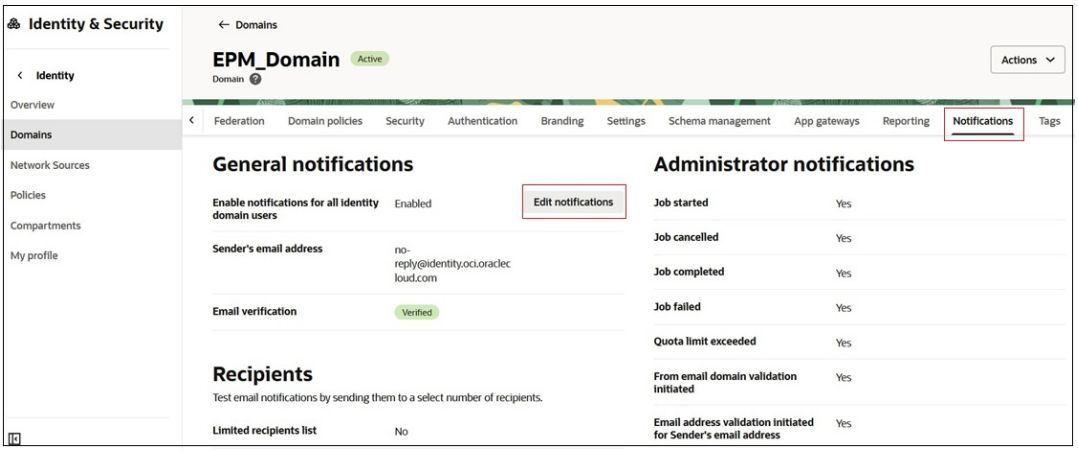
Make sure that Federated and ByPass Notification fields are both set to TRUE.

How to Avoid Welcome Emails for Users Created Through Cloning

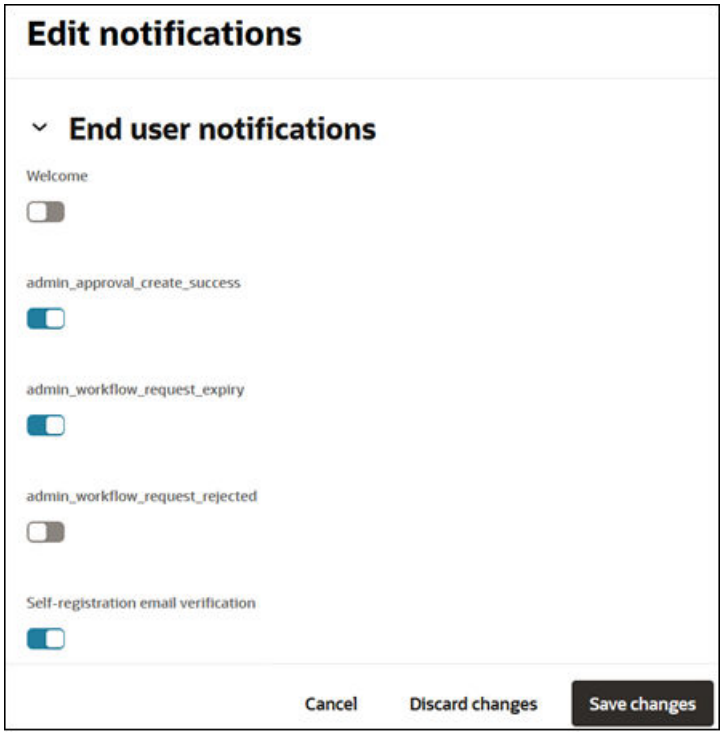
In SSO-enabled environments, you can prevent activation emails being sent to newly created users through the cloning process, for example, during the migration to OCI (Gen2). For more information, see Customize Oracle Identity Cloud Service Notifications.

To turn off activation emails:

1. Sign into IAM Interface. See: Accessing the IAM Interface.
2. Navigate to **Notifications** tab.
3. Click **Edit notifications**.



4. On **Edit notifications** page, scroll down to **End User notifications**.
5. Disable the notifications you do not wish to send.



6. Click **Save changes**.

Setting Password Policies

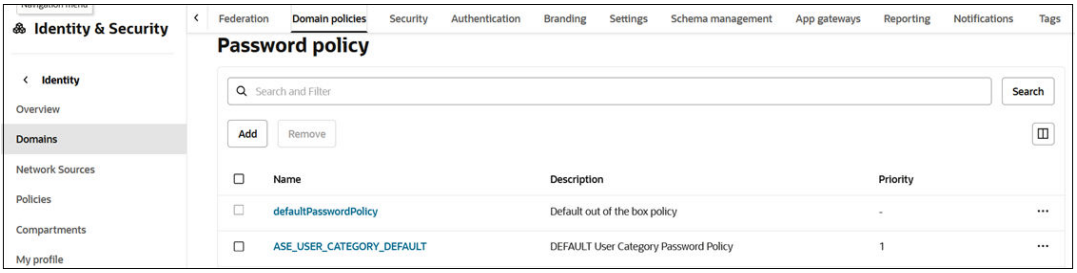
You have the option to establish up to ten password policies within IAM Interface, each designated with a priority. A password policy is assigned to a group, and all users in the group will use that policy. When a user belongs to multiple groups, the password policy with the highest priority is enforced.

When a user is created or modifies their password, IAM validates the provided password against the highest priority password policy applicable to that user, ensuring compliance with the policy criteria:

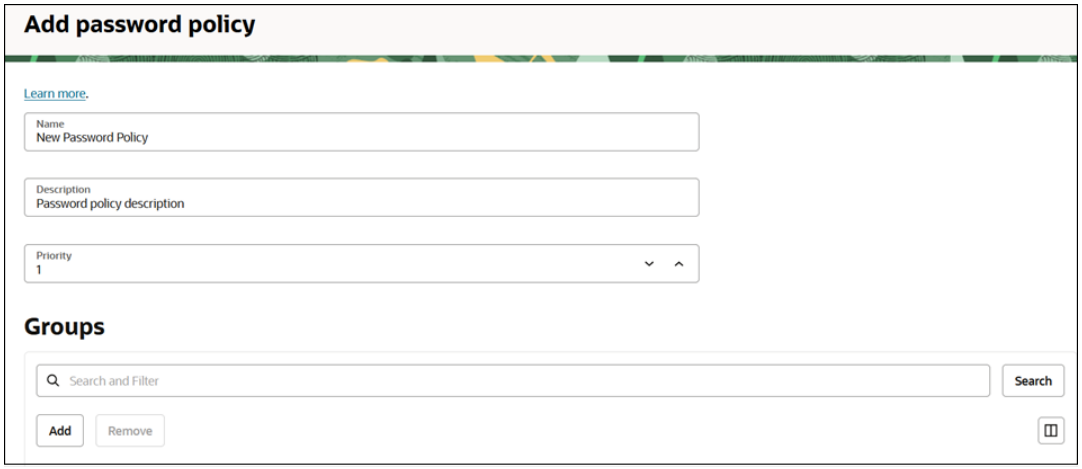
- A new user who is not a member of a group will use the default password policy.
- Similarly, a user belonging to a group without an assigned password policy will also use the default password policy.
- When a user logs in for the first time to change the password, or resets the password at any time, the password policy is evaluated.

Setting Password Policies

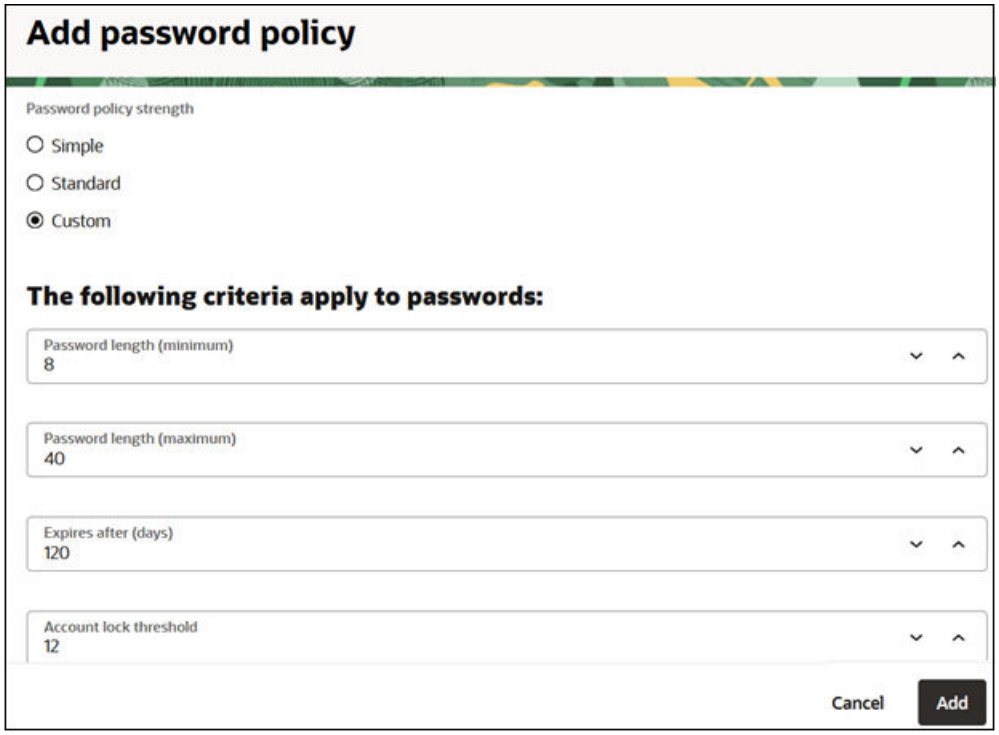
1. Sign into IAM Interface as an Identity Domain Administrator. See: Accessing the IAM Interface.
2. Navigate to **Domain policies** tab.
3. Scroll-down to Password policy section. Click **Add**.



4. On **Add password policy** page, enter the **Name** and **Description**.



5. Select the **Priority** value.
The priority can be any integer between 1 and 10, where 1 is highest priority and 10 is lowest. If there is already a password policy with the priority you choose, that policy moves to the next priority number. For example, if there is a password policy with a priority of 2 and another with a priority of 3, and you create a new policy with a priority of 2, the other policies will have priorities of 3 and 4.
6. To add one or more groups to the password policy, click **Add**, select the groups, and then click **Add**.
Each group can only have one policy assigned to it.
   - If a user has only one group assigned to them, then the password policy assigned to that group is the password policy assigned to the user.
   - If a user has more than one group assigned to them, then the password policy with the highest priority is the password policy assigned to the user.
7. Select the type of password policy: **Simple**, **Standard**, or **Custom**.
If you select **Simple** or **Standard**, the criteria for the selected policy are displayed. You can't change the criteria for these policies. If you select **Custom**, you can customize the criteria.



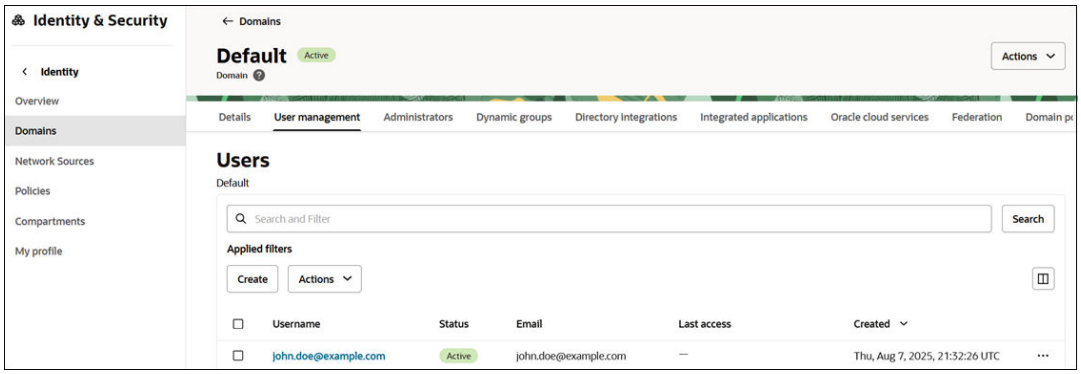
8. Select the password criteria, including character requirements and any specific options the password must contain.
9. When you're finished, click **Add**.

Resetting User Password

Identity Domain Administrators can reset user's password. When the password reset is successful, the system automatically generates a new temporary password and mails it to the user. Users are required to change the temporary password the next time they sign in.

To reset user password:

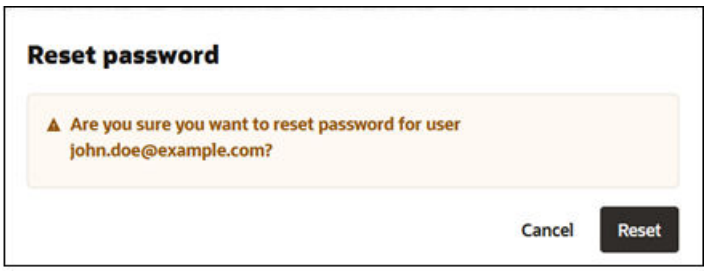
1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Navigate to **User management** tab.



3. To reset password for a user -

a. Click **ellipses** next to the user account, and select **Reset Password**

b. Click **Reset**. A password reset notification is sent to the user account.

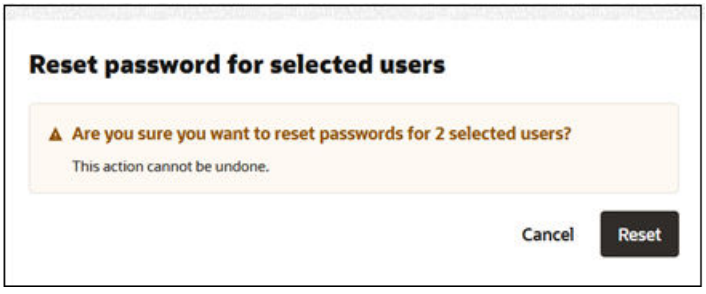


4. To reset passwords for selected users -

a. Check the box next to each user account you want to include.

b. Click **Actions** and select **Reset password for selected users**.

c. Click **Reset**. A password reset notification is sent to the selected user accounts.

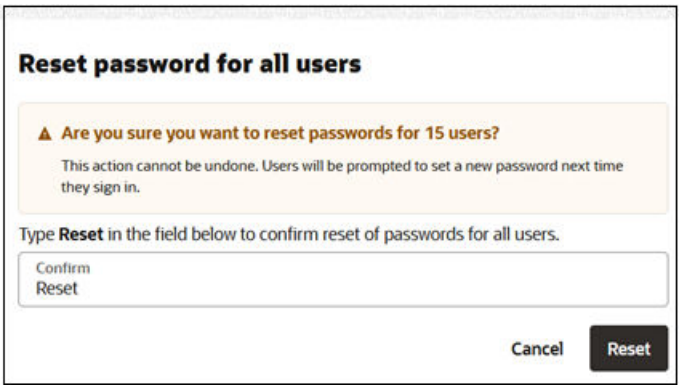


5. To reset passwords for all users -

a. Click **Actions** and select **Reset password for all users**

b. Enter *Reset* to confirm reset of passwords for all users.

c. Click **Reset**. A password reset notification is sent to all user accounts.



Audit and Login Reporting Overview

Access and Permissions

- Users assigned the Identity Domain Administrator role can view both audit reports and login reports
- Service Administrators also have access to the Role Assignment Audit Report

Audit Data Retention Periods

The default retention period for audit data is 30 days, configurable up to 90 days using the **Audit Retention Period (days)** setting in the Oracle Cloud Console. This setting applies to the following:

- Role Assignment Audit Report
- Invalid Login Report

Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management maintains the audit data displayed for the following reports for a maximum of 120 days:

- Group Assignment Audit Report
- User Login Report

Custom Date Range Reporting

Reports can be generated for a custom date range, subject to the following rules:

- The start date must not be earlier than the allowed maximum retention period from the current date.
- The end date must not be later than the maximum retention period from the start date.
- The end date must be later than the start date.

Archiving Reports

To retain audit data for more than the audit data retention period, it is recommended to periodically download and archive the reports. All reports can be exported in CSV format.

Available Audit and Login Reports

- Available Audit Reports

- Available Login Reports

Available Audit Reports

The following audit reports are available:

- In Oracle Cloud Console:
  - Application Access Report
  - Application Role Privileges Report
- In Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management:
  - Role Assignment Audit Report
  - Application Audit Report
  - Group Assignment Audit Report

> **Note**
>
> All columns in these reports are **sortable**. For example, in the Application Access Report, you can click the sort button in the **User** column to organize the data alphabetically.

Application Access Report

Provides login details, including:

- **User**: Name of the user who logged in
- **Login**: Email address of the user who logged in
- **Message**: Whether the login attempt was successful
- **Application**: Name of the application accessed
- **Date**; UTC timestamp (24-hour format) when the action occurred

For steps on generating these reports. See Accessing Audit Log Report in Oracle Cloud Console

Application Role Privileges Report

Tracks changes made to predefined roles. This report serves as an audit trail for all predefined role modifications. Each row includes:

- **User**: Name of the administrator who assigned or unassigned the role
- **Application Name**: Name of the environment for which the role was assigned or unassigned
- **Beneficiary:** User assigned or unassigned a role
- **Type**: Type of user
- **Application Role Name**: Name of the predefined role assigned or unassigned
- **Message**: Whether the predefined role was assigned or unassigned to the user
- **Date**; UTC timestamp (24-hour format) when the action occurred

For steps on generating these reports. See Accessing Audit Log Report in Oracle Cloud Console

Role Assignment Audit Report

Tracks changes to predefined and application role assignments within your environment. Each row includes:

- **Name**: Name of the user, IDCS group, or EPM group associated with the role change
- **Type**: Whether it is a user, IDCS group, or EPM group
- **Role**: The specific predefined or application role that was assigned or unassigned
- **Action**: Whether the role was assigned or unassigned
- **Performed By**: User who made the role change
- **Date and Time**: UTC timestamp (24-hour format) when the action occurred

You can generate this report using:

- roleAssignmentAuditReport EPM Automate command
- Role Assignment Audit Report REST API

Application Audit Report

Audits tasks performed by users. You can filter audited tasks by audit type (for example, Data, Approvals, or Clear Cell Details), date range (for example, Yesterday or Last 60 Days), and user name. Each row includes:

- **Audit** - Tasks enabled for auditing
- **Source** - Source of the task. For example, Balance Sheet, Vision
- **Action** - Action performed on the task. For example, executed or modified
- **User** - ID of the user who performed the task
- **Name** - Name of the user who performed the task
- **Date** - UTC timestamp (24-hour format) when the action occurred
- **Details** - Information on the task audited
- **Property** - Property associated with the task
- **Old Value** - Old value of the property before the task was performed
- **New Value** - New value of the property after the task was performed

You can generate this report using:

- exportAppAudit EPM Automate commmand
- Export Audit *REST API*
- Viewing Audit Details via Audit tool for Cloud EPM platform applications

Group Assignment Audit Report

Lists users and groups added to or removed from EPM groups within a specified date range (up to 120 days). Each row includes:

- **User/Group Name**: Name of the user or group
- **User/ Group Type**: Either IDCS, predefined, or EPM group

- **Action**: Whether the user or group is assigned to the EPM group
- **Group**: EPM group name
- **Group Type**: EPM
- **Performed By**: Service Administrator who performed the action
- **Date and Time**: UTC timestamp (24-hour format) when the action occurred

You can generate this report using:

- groupAssignmentAuditReport EPM Automate command
- Group Assignment Audit Report REST API

Available Login Reports

The following audit reports are available:

- In Oracle Cloud Console:
  - Successful Login Attempts Report
  - Unsuccessful Login Attempts Report
  - Dormant Users Report
- In Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management:
  - User Audit (User Login) Report
  - Invalid Login Report

Successful Login Attempts Report

Displays details of successful user logins, including:

- **Login**: User ID of the person who signed in
- **Provider**: Authentication method used (for example, `UserNamePassword` or the name of a SAML provider)
- **Date**: UTC timestamp (24-hour format) when the login occurred

For steps on generating these reports. See Accessing Audit Log Report in Oracle Cloud Console.

Unsuccessful Login Attempts Report

Lists failed login attempts with the following details:

- **User Name:** Name of the user who attempted to sign in
- **IP Address:** Remote IP address from which the user attempted to sign in
- **Timestamp**: UTC timestamp (24-hour format) when the action occurred

For steps on generating these reports. See Accessing Audit Log Report in Oracle Cloud Console.

Dormant Users Report

Identifies users who have not signed in during a selected period:

- **User Name**: User ID of the user who has not signed in during the selected period

- **Last Successful Login Date**: Date of last login
- **Full Name**: Full name of the dormant user
- **Primary Email**: Primary email address of the dormant user

For steps on generating these reports. See Accessing Audit Log Report in Oracle Cloud Console.

User Audit (User Login) Report

Contains information on the users who signed into the environment over a specified time period:

1. **User Login**: User ID of the user who signed in
2. **IP Address**: Remote IP address from which the user signed in
3. **Access Date and Time**: UTC timestamp (24-hour format) when the login occurred

You can generate this report using:

- Viewing the User Login Report via Access Control tool
- userAuditReport EPM Automate command
- User Audit Report REST API

Invalid Login Report

Lists the unsuccessful login attempts to sign into the environment over a specified time period:

1. **User Name**: User ID of the user who attempted to sign in
2. **IP Address**: Remote IP address from which the user attempted to sign in
3. **Access Date and Time**: UTC timestamp (24-hour format) when the login attempt occurred

You can generate this report using:

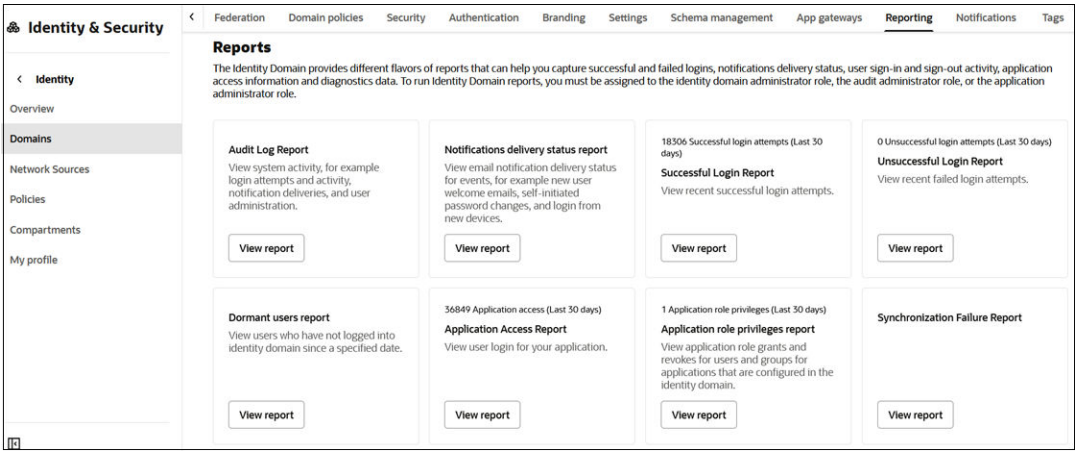
- invalidLoginReport EPM Automate command
- Invalid Login Report REST API

Accessing Audit Log Report in Oracle Cloud Console

The IAM Interface provides different flavors of reports that can help you capture successful and failed logins, notifications delivery status, user sign-in and sign-out activity, application access information and diagnostics data.

Audit and Login reports are generated for the audit retention period of 30 (default), 60 or 90 days as specified in default settings of your identity domain. See Setting the Audit Retention Period in *Oracle Cloud Infrastructure Documentation*.

1. Sign into IAM Interface as an Identity Domain Administrator in the source domain. See: Accessing the IAM Interface.
2. Navigate to **Reporting** tab.



3. Under Audit Log Report, click **View report**.
4. On the report page, enter filter values, such as dates and event identifiers, to search for specific information.
5. Download the results by selecting **Download report**.
   The report is created and saved at the location you select or opened in Excel

Accessing Audit Reports Using Identity Cloud Service REST APIs

Using the Audit Events REST endpoints, Identity Domain Administrator can utilize Oracle Identity Cloud Services audit event data to complete these tasks:

- Generate reports of users' activities
- Capture historical user activities
- Analyze application usage

See the following information sources in *REST APIs for Oracle Fusion Cloud EPM*:

- Using the Audit Event APIs for detailed information on audit events REST endpoints.
- Search Audit Events for information on Search by GET action.

To access audit and user reports using Identity Cloud Service REST APIs, you need to complete these steps:

- Set up authentication with OAuth 2 for your REST client to get refresh token and Client ID
- Use the refresh token and Client ID to get the access token to issue the REST API to IDCS

For information on completing these tasks, see Authentication with OAuth 2 - Only for OCI (Gen 2) Environments in *REST APIs for Oracle Fusion Cloud EPM*.

Accessing IDCS audit endpoints requires `urn:opc:idm:__myscopes__` scope.

Table 7-1 IDCS Audit Event Endpoints

Action	Method	Endpoint
Search by GET	GET	`/admin/v1/AuditEvents`
Search by POST	POST	`/admin/v1/AuditEvents/.search`
Get by Event id	GET	`/admin/v1/AuditEvents/{id}`

Elaborate search queries can be constructed using the following:

- Filter parameters to select events based on attributes (see SCIM specifications)
- Attributes to filter and to return
- Sort to sort results and set sort order
- Count to limit the number of events per page
- Start index to support pagination (see SCIM specifications)

Accessing Usage Reports

The Usage Report contain the usage metrics for the Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment. It shows what you licensed, how much you licensed, how much you're using, and if you're using more than what you licensed.

Required Permission to View Reports

Usage reports are stored in an Oracle Cloud Infrastructure Object Storage bucket. To access the location where the documents are stored, you need to set up a cross-tenancy policy. You must be a member of a group with these necessary policy permissions to view the reports :

```
Define tenancy usage-report as
ocid1.tenancy.oc1..aaaaaaaaned4fkpkisbwjlr56u7cj63lf3wffbilvqknstgtvzub7vhqkgg
q
Endorse group '<identity-domain-name'/'<your-group-name>' to read objects in
tenancy usage-report
Allow group '<identity-domain-name'/'<your-group-name>' to read organizations-
subscriptions in tenancy
Allow group '<identity-domain-name'/'<your-group-name>' to read subscriptions
in tenancy
Allow group '<identity-domain-name'/'<your-group-name>' to read organizations-
assigned-subscriptions in tenancy
Allow group '<identity-domain-name'/'<your-group-name>' to read organizations-
subscription-regions in tenancy
```

To create a policy, see Creating Policies for Users and Groups.

Viewing the Reports

To view the usage reports:

1. Sign in to the Oracle Cloud Console.
2. Open the navigation menu and click **Billing & Cost Management**.
3. Under **Billing**, click **Subscriptions**. Alternatively, On the **Applications home** page, under **Quick actions**, click **View subscriptions**.
4. Click a subscription name to view the **Subscription information**.
5. Under **Resources**, click **Usage** for this subscription.
6. Select the usage report name to download the pdf file.

8

Configuring Security Settings

You can use the default Single Sign-On (SSO) or use a Security Assertion Markup Language 2 (SAML 2) compliant identity provider (IdP) to authenticate users to multiple business processes.

In This Section:

Configuring Single Sign-On

You can configure SSO to enable users belonging to a SAML 2.0 compliant identity provider (IdP) to authenticate against many Oracle cloud environments.

> **Note**
>
> Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management support only Service Provider (SP) initiated SSO; it does not support IdP initiated SSO.

Users use the SSO credentials to access network resources of their organization to authenticate once to an environment, and then seamlessly access other cloud environments configured using the same IdP.

You may use any SAML 2.0IdP, for example, Microsoft Entra ID, Oracle Identity Federation, Microsoft Active Directory Federation Services 2.0+, Okta, Ping Identity PingFederate, and Shibboleth, to establish SSO.

> **Note**
>
> The information in this section does not apply to SaaS at Customer (Cloud EPM and Cloud EDM deployed within a customer cloud).

This section covers the following topics:

- Configuring Microsoft Entra ID for SSO
- Configuring Multiple Identity Providers for a Single Domain
- Configuring SSO Between Services Across Identity Domains within an Oracle Cloud Account

Configuring Microsoft Entra ID for SSO

Refer to the steps in the links below to configure and enable the use of Microsoft Entra ID (Azure AD), a SAML 2.0 compliant identity provider (IdP) to establish SSO for your Cloud EPM and Cloud EDM environments:

- Steps to Complete in Microsoft Entra ID and
- Steps to Complete in Oracle Cloud Console

Troubleshooting

See Resolving Login Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*

Steps to Complete in Microsoft Entra ID

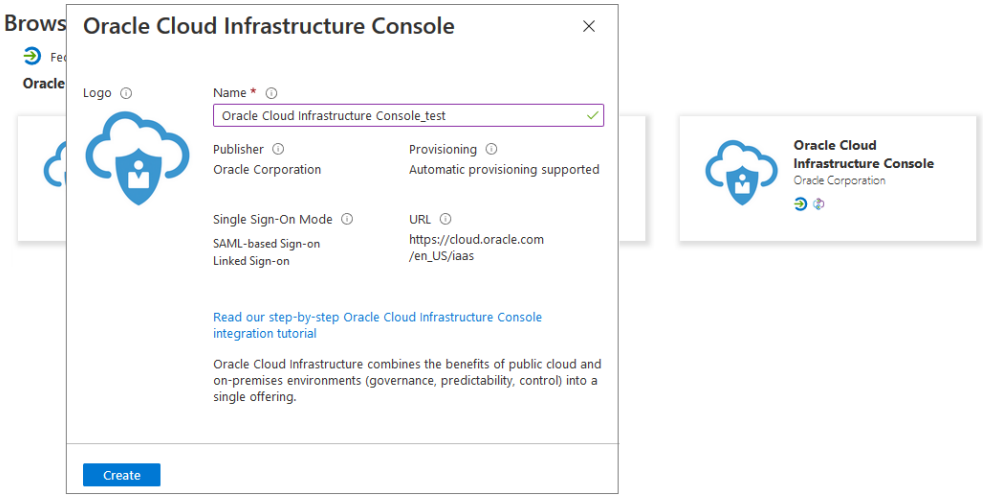
To configure Microsoft Entra ID as an identity provider (IdP), complete these actions:

1. Add Oracle Cloud Infrastructure Console as an enterprise application in Azure AD.
2. Assign Azure AD users to the Oracle IDCS enterprise application.
3. Setup SSO for the Oracle Cloud Infrastructure Console Enterprise Application.

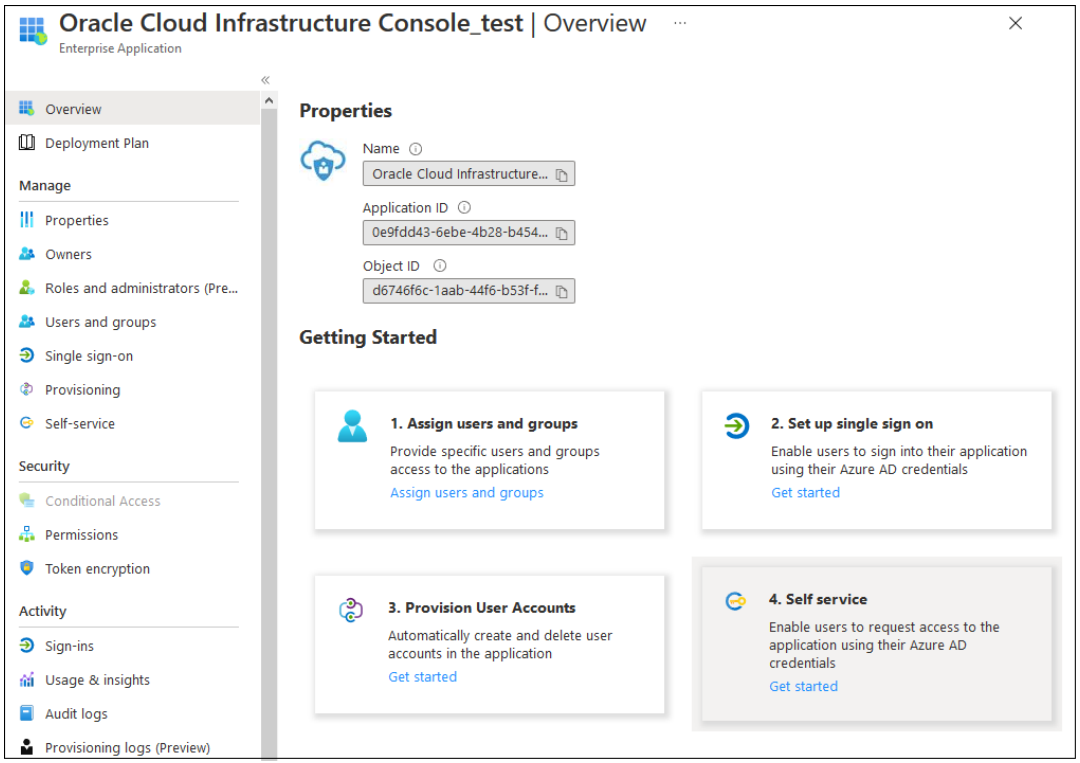
Refer to Microsoft Entra ID documentation for detailed steps and explanation related to completing these configuration steps.

Add Oracle Cloud Infrastructure Console as an Enterprise Application

1. Access Microsoft Entra ID sign-in page and sign in.
2. On the Home left-navigation pane, click **Applications**, and then click **Enterprise applications**.
3. Click **New application**. Browse **Microsoft Entra Gallery** screen, which lists Oracle as a cloud platform.
4. Click **Oracle** to display a list of available Oracle Cloud platforms.
5. Click **Oracle Cloud Infrastructure Console**.



6. Enter a **Name**, and then click **Create** to add an instance of Oracle Cloud Infrastructure enterprise application.
An overview of the enterprise application properties is displayed.



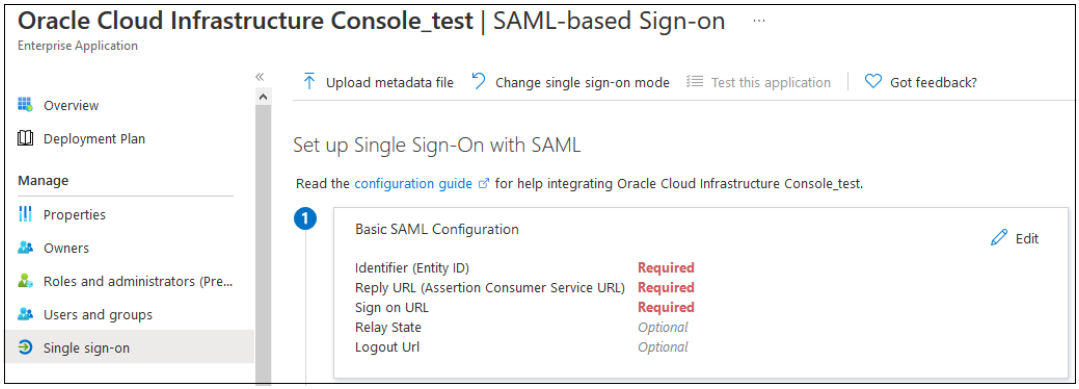
Assign Microsoft Entra ID Users to Oracle Cloud Infrastructure Console Enterprise Application

Only the specified users can log in to Microsoft Entra ID and be federated with Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management . You can also assign user groups. Ensure that these users or groups are already present in Microsoft Entra ID.

1. In the left navigation pane of your Oracle Cloud Infrastructure Console application, click **Users and groups** under **Manage**. Alternatively, in the Overview page of your enterprise application, click **Assign users and groups**.
2. Click **Add user/group**.
3. Under **Users**, click **None Selected** to open the **Users** screen. Select the users to assign to the application and click **Select**.
4. Click **Assign** to assign the selected users to the application.

Setup SSO for the Oracle Cloud Infrastructure Console Enterprise Application

1. In the left navigation pane, click **Single sign-on**
2. In **Select a single sign-on method**, click **SAML**.
   The **Set up Single Sign-on with SAML** screen opens.



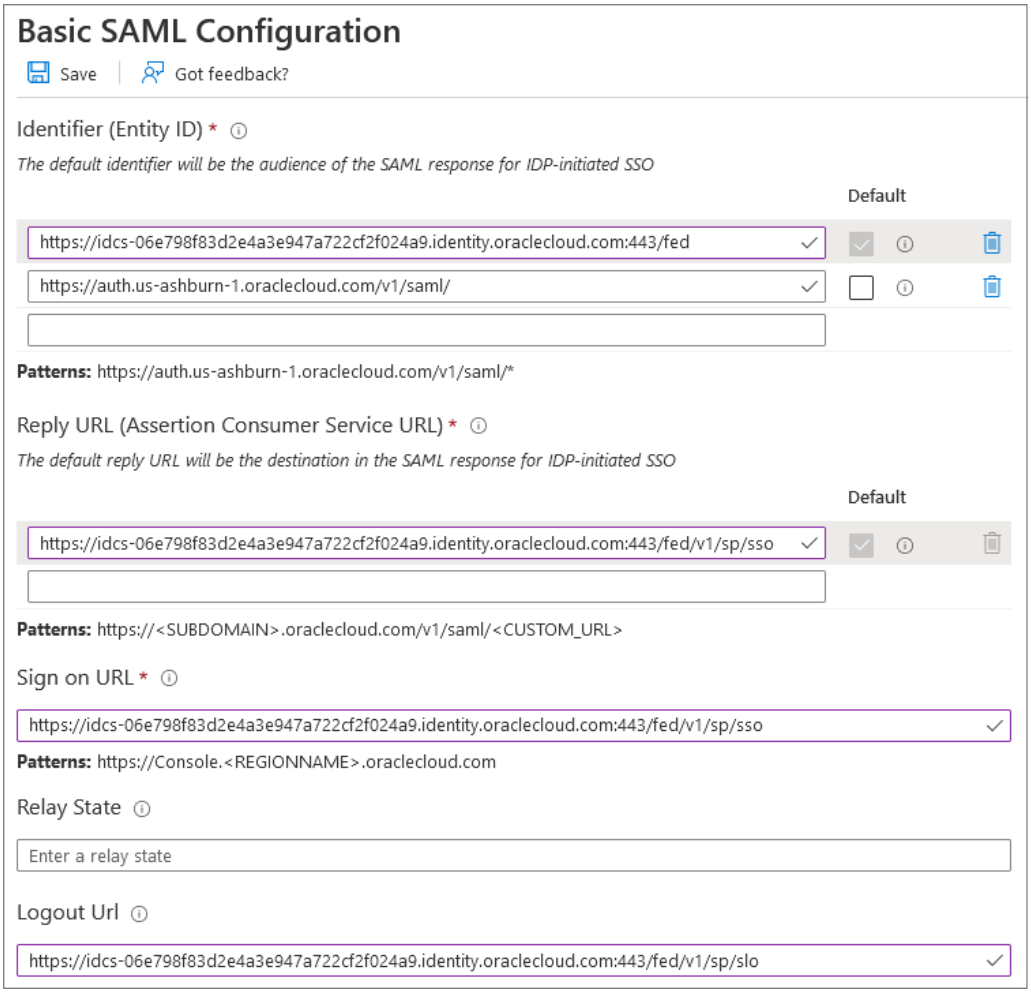
3. Enter basic SAML configuration details.
   The information that you should enter in this step is generated while configuring SAML in Oracle Identity Cloud Service.
   - Click **Edit** in **Basic SAML Configuration** section.
   - In **Basic SAML Configuration** page, enter settings to SSO with your Oracle Identity Cloud Service.

> **Note**
>
> The Oracle Identity Cloud Service settings that you need to enter as basic SAML settings follow this predictable pattern. `https://idcs-CUSTOMER_IDENTIFIER.identity.oraclecloud.com:443/fed` The *CUSTOMER_IDENTIFIER* is a unique alphanumeric string specific to your tenancy. It is a part of the Oracle Identity Cloud Service URL. For example, if the sign in URL is `https://idcs-01e711f676d2e4a3e456a112cf2f031a9.identity.oraclecloud.com/ui/v1/signin`, the *CUSTOMER_IDENTIFIER* is `01e711f676d2e4a3e456a112cf2f031a9`, which you use to derive the SAML configuration settings. In this example, the Identifier (Entity ID) would then be `https://idcs-01e711f676d2e4a3e456a112cf2f031a9.identity.oraclecloud.com:443/fed`.
>
> To view all well known Oracle Identity Cloud Service configuration settings for your tenancy, enter your Oracle Identity Cloud Service URL appended with `/.well-known/idcs-configuration`. For example, `https://idcs-01e711f676d2e4a3e456a112cf2f031a9.identity.oraclecloud.com/.well-known/idcs-configuration`.

- **Identifier (Entity ID):** The Provider ID that was set while provisioning Oracle Identity Cloud Service for your organization.
  Example: `https://idcs-CUSTOMER_IDENTIFIER.identity.oraclecloud.com:443/fed`

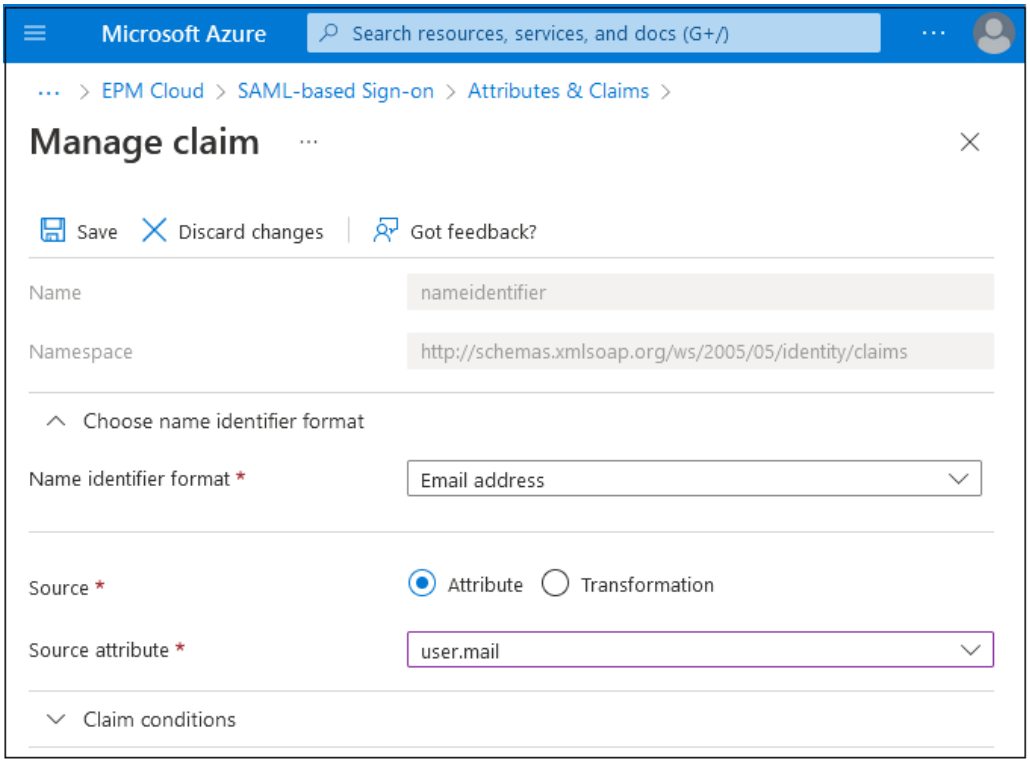
  > **Note**
  >
  > Select the **Default** check box to indicate that this is the default identifier.

- **Reply URL:** The endpoint in Oracle Identity Cloud Service that will process incoming SAML assertions from Microsoft Entra ID. Also known as Assertion Consumer Service URL, this value is set while configuring Oracle Identity Cloud Service.
  Example: `https://idcs-CUSTOMER_IDENTIFIER.identity.oraclecloud.com:443/fed/v1/sp/sso`
- **Sign on URL:** The URL of the Cloud EPM and Cloud EDM sign on page that performs the SSO initiated by Microsoft Entra ID.
  Example: `https://idcs-CUSTOMER_IDENTIFIER.identity.oraclecloud.com:443/fed/v1/sp/sso`
- **Logout URL:** The logout service URL from Oracle Identity Cloud Service.
  Example: `https://idcs-CUSTOMER_IDENTIFIER.identity.oraclecloud.com:443/fed/v1/sp/slo`



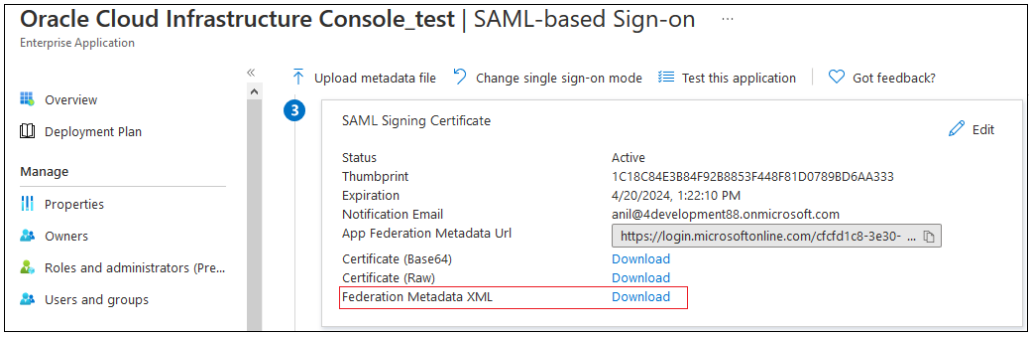
- Click **Save**.
- Close the **Basic SAML Configuration** page

4. In **Set up Single Sign-On with SAML** screen, enter user attributes and claims:
   - Click **Edit** in **Attributes & Claims**.
   - Under **Claim name**, click **Unique User Identifier (Name ID)**, select a source attribute value, for example, **user.mail**. This value should match the *Requested NameID* format specified in Oracle Identity Cloud Service.



- Click **Save**.
- Close the **Manage claim** and **Attributes & Claims** pages.

5. Download the Microsoft Entra ID metadata file.
   - In the **Set up Single Sign-On with SAML** screen, in the **SAML Signing Certificate** section, click **Download** next to **Federation Metadata XML**.



- Follow the on-screen prompts to save the metadata file to a local directory that is accessible from Oracle Identity Cloud Service.

Steps to Complete in Oracle Cloud Console

For each account for which you want to set up SSO, complete these actions:

1. Manage Oracle Fusion Cloud Enterprise Performance Management users
2. Setup Azure AD as a SAML IdP and Assign to an IdP Policy

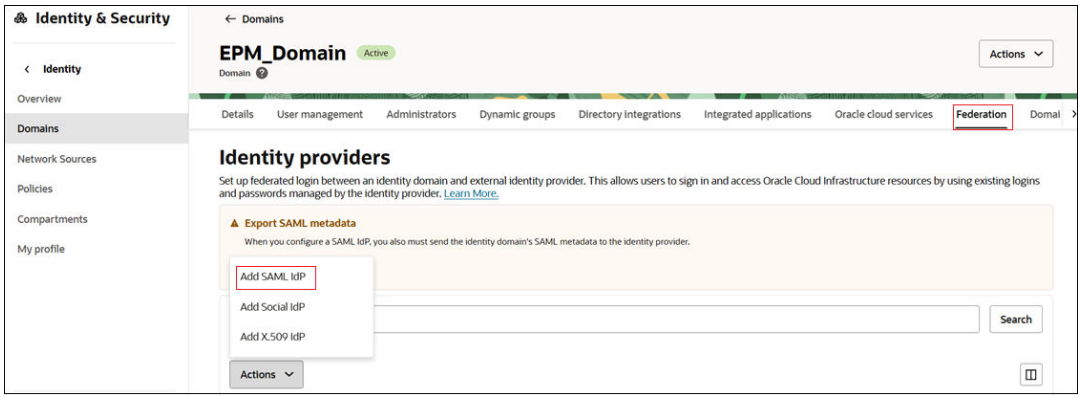
Manage Users

1. Create users. See Creating User
2. Assign users to predefined roles. See Assigning Roles.

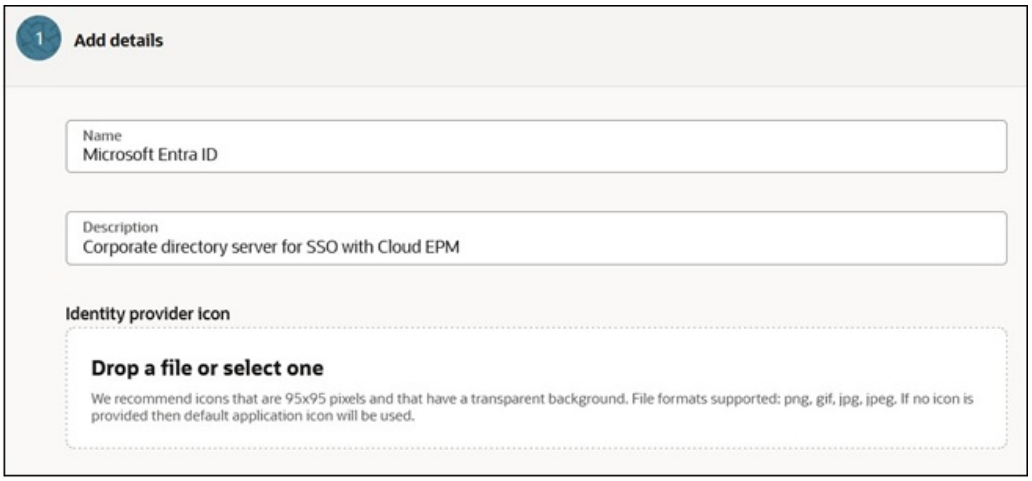
Setup Microsoft Entra ID as a SAML IdP and Assign to an IdP Policy

For detailed instructions on this task, see Add a SAML Identity Provider in *Oracle Cloud Infrastructure Documentation.*

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to the **Federation** tab.
3. Click **Actions**, select **Add SAML IdP** and submit the tasks in the workflow.

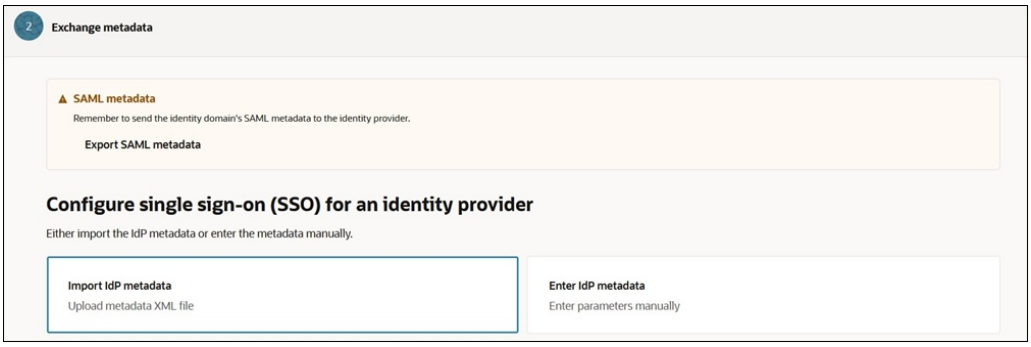


4. **Task 1 - Add details:**
   - **Name**: Enter the name of the SAML IdP.
   - (Optional) **Description**: Enter a description of the IdP.
   - (Optional) **Identity provider icon**: Drag and drop a supported image, or click **select one** to browse for the image.

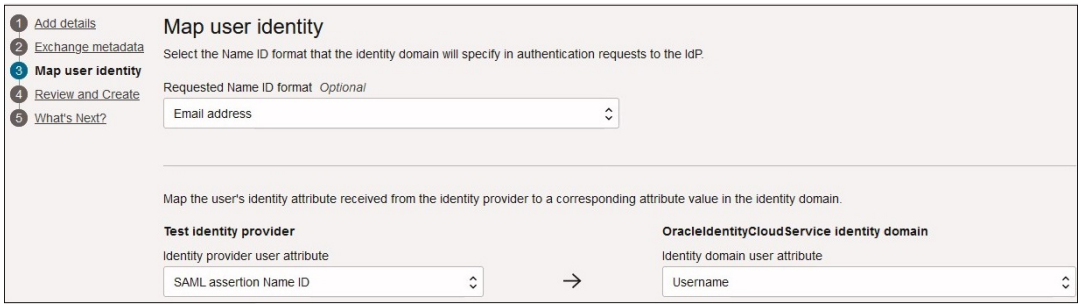


5. Click **Next**.

6. **Task 2 - Exchange metadata:**
   a. Click **Export SAML metadata** button to send the SAML metadata to Microsoft Entra ID.
   b. Select **Import IdP metadata**.
   c. Browse and select the Microsoft Entra ID metadata file that you downloaded. See Steps to Complete in Microsoft Entra ID.



7. Click **Next**.
8. **Task 3- Map user identity**. map user's identity attributes received from Microsoft Entra ID to an Oracle Cloud Infrastructure identity domain.



   - For **Requested NameID Format**, select the format in which Microsoft Entra ID forwards the user attribute to Oracle Identity Cloud Service.
   - For **Test identity provider**, select the Microsoft Entra ID attribute that uniquely identifies the user. To use an attribute other than user ID (for example, email ID), select **SAML Attribute**. Otherwise select **Name ID**.
   - For **OracleIdentityCloudService identity domain**, select the Oracle Identity Cloud Service attribute to which you want to map the Microsoft Entra ID attribute that you selected.

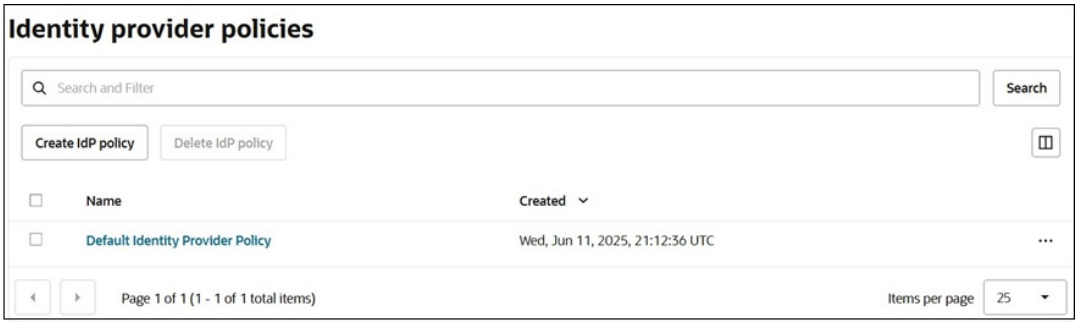
9. Click **Next**.
10. On the **Review and Create** page, verify the entered details. Click **Create IdP**.
11. Under **Identity Providers**, click Microsoft Entra ID
12. On the Microsoft Entra ID details page, verify SAML SSO.
    a. Using the Identity Provider's **Actions** menu, select **Test Login** from the menu.

b. Authenticate with your credentials to test the connection.
If successful, a message will appear: **"Your connection is successful."**

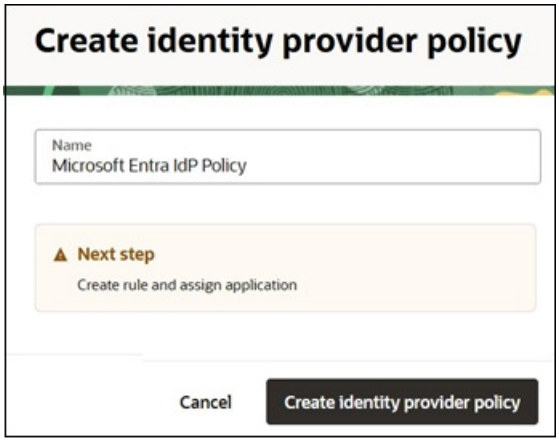
13. Activate Microsoft Entra ID so that the identity domain can use it. Using **Actions** menu, select **Activate IdP**.
14. Assign Microsoft Entra ID to an existing policy rule you have created. Using **Actions** menu, select **Add to IdP policy**. If you plan to create a policy and then assign a rule, see Create an IdP Policy and Assign Rule.

Create an IdP Policy and Assign Rule

1. On the **Federations** tab, scroll-down to **Identity providers policies**.
2. Click **Create IdP policy**.

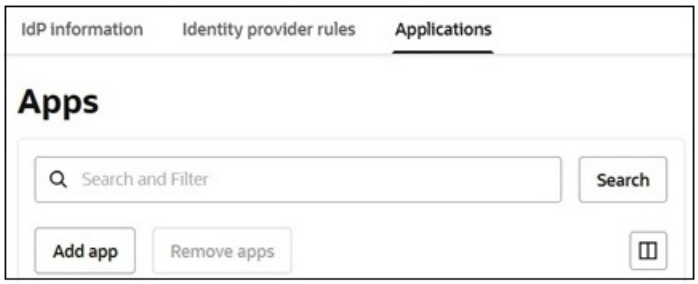


3. On the **Create identity provider policy** page, enter the **Name** and then click **Create identity provider policy**.



4. Navigate to **Identity provider rules** tab.
5. Click **Add IdP rule** to define rules for this policy.

6. On **Add identity provider rule** page:
   a. Enter a **Rule name**.
   b. Use the **Assign identity providers** menu to assign Microsoft Entra ID to this rule.
   c. Configure conditions.
   d. Click **Add IdP rule**.
7. Assign application to this policy. Navigate to **Applications** tab.
8. Click **Add apps**.



9. On the **Add app** page:

a. Search and select the apps to assign to this IdP policy.

b. Click **Add App**.
You can now SSO to these environments using any of the configured IdPs.

Configuring Multiple Identity Providers for a Single Domain

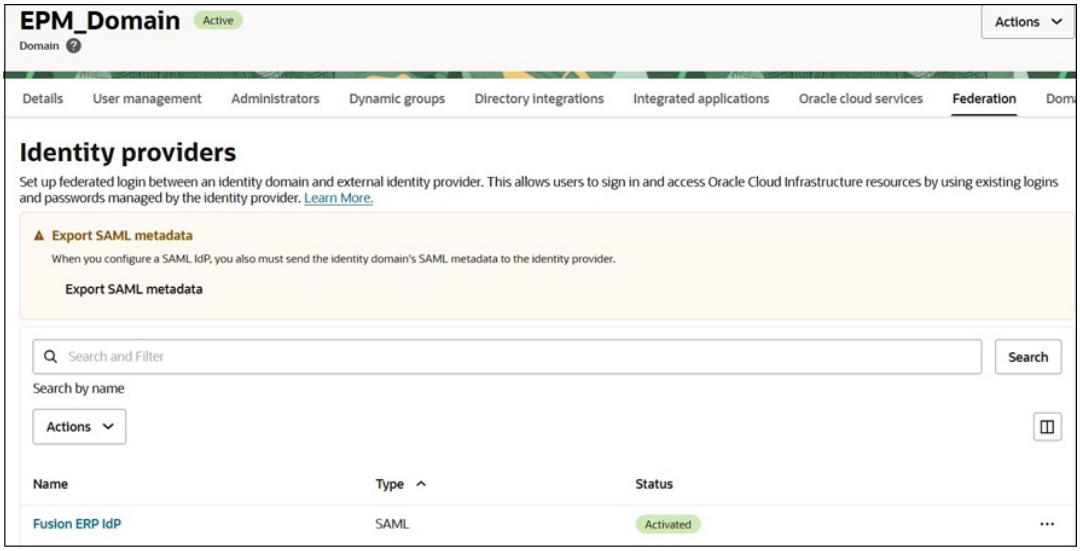
You can configure to use multiple identity providers (IdPs) to provide Single Sign-On (SSO) access to the users. If multiple IdPs are enabled for an environment, the **Sign In** page allows users to choose the IdP to perform SSO.

To configure an IdP, refer to this Microsoft Entra ID setup example:

- Steps to Complete in Microsoft Entra ID
- Steps to Complete in Oracle Cloud Console

Activate and Enable the IdPs

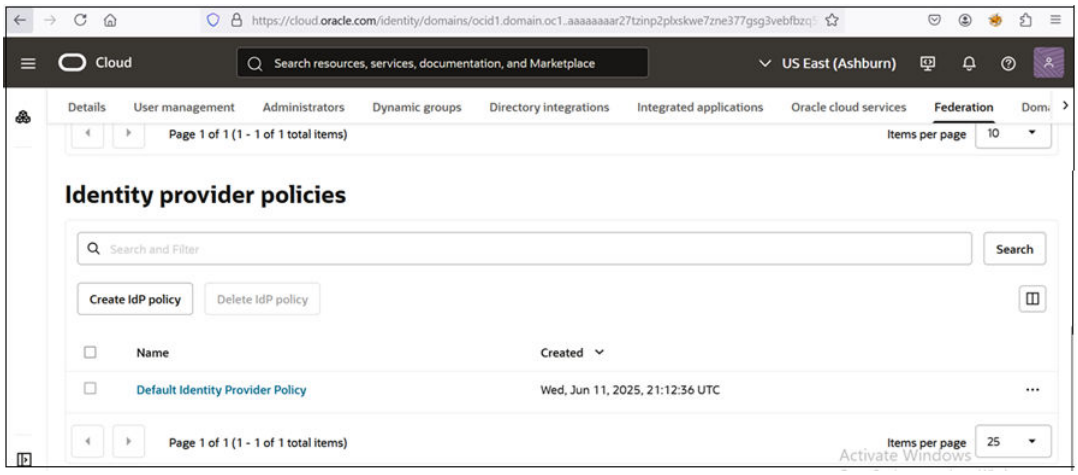
1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to the **Federation** tab. The Identity Providers in the domain are listed.



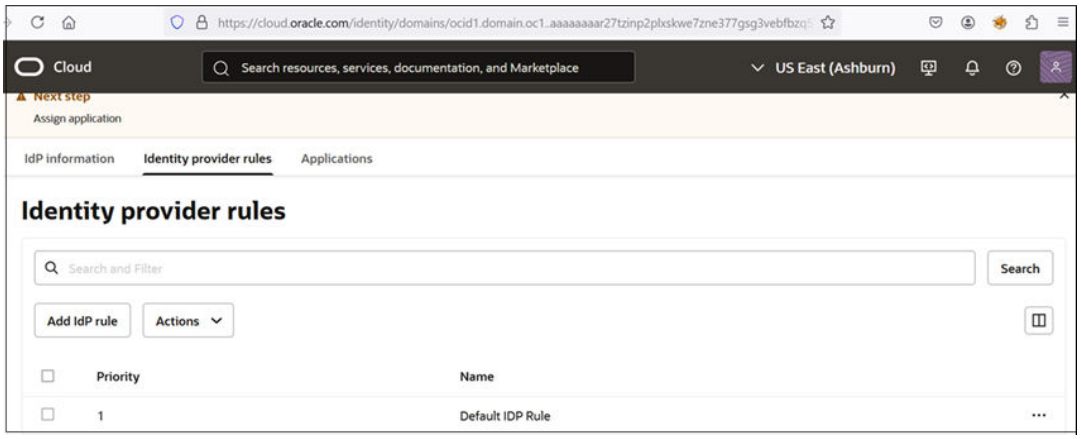
3. Select the identity provider that you wish to activate. Click the **Ellipses** menu (three dots) for the IdP that you want to activate and select **Activate IdP**.
4. To confirm the activation, click **Activate IdP**.

Assign IdP Rule to Multiple IdPs

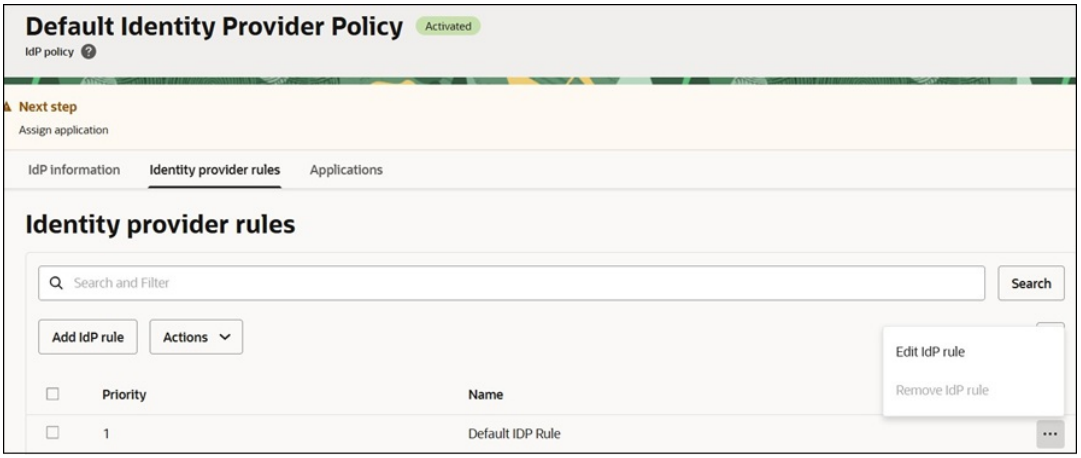
1. Scroll-down to **Identity Provider policies**.
2. Click the name of the IdP policy to assign an IdP rule.



3. Navigate to **Identity provider rules** tab.

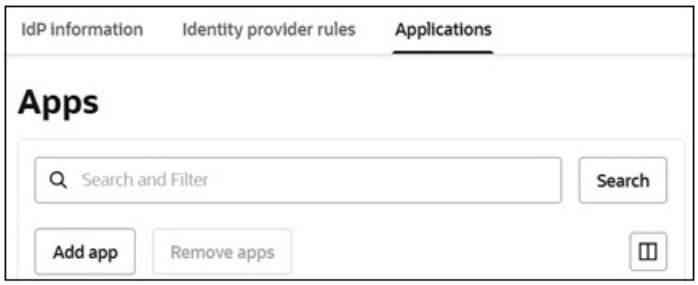


4. Click **Ellipses ...** next to the IdP policy rule, and then and select **Edit IdP rule** from the menu.



5. On **Edit Identity Provider rule** page, use the **Assign identity providers** menu to assign IdP to this rule.
6. When you are finished, click **Save changes**.

7. Assign application to this policy. Navigate to **Applications** tab.
8. Click **Add app**.



9. On the **Add app** page:
   a. Search and select the apps to assign to this IdP policy.
   b. Click **Add App**.

   You can now SSO to these environments using any of the configured IdPs.

Configuring SSO Between Services Across Identity Domains within an Oracle Cloud Account

Within a single Oracle Cloud account, you may have multiple services deployed across different identity domains. To provide a seamless user experience, you can configure Single Sign-On (SSO) between these identity domains.

Example Scenario

Suppose you're using the Oracle Fusion Suite, which includes Fusion ERP and Oracle Fusion Cloud Enterprise Performance Management services, each set up in separate identity domains. You can enable seamless cross-domain access by setting up SSO between them:

- Fusion ERP serves as the Identity Provider
- Cloud EPM functions as the Service Provider

In this topic, we'll walk through how to configure SSO for this scenario:

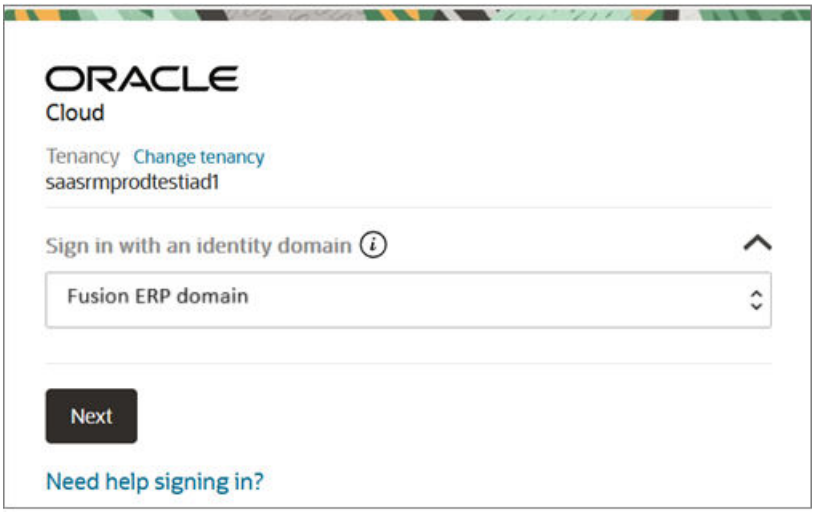
- Step 1 - Open Separate Sessions for Each Domain
- Step 2 - Fusion ERP Domain - Download Fusion ERP Metadata
- Step 3 - EPM Domain - Configure Fusion ERP as an Identity Provider
- Step 4 - Fusion ERP Domain - Add Cloud EPM as an Integrated Application
- Step 5 - EPM Domain - Verify SAML SSO
- Step 6 - Fusion ERP Domain - Test SSO

Step 1 - Open Separate Sessions for Each Domain

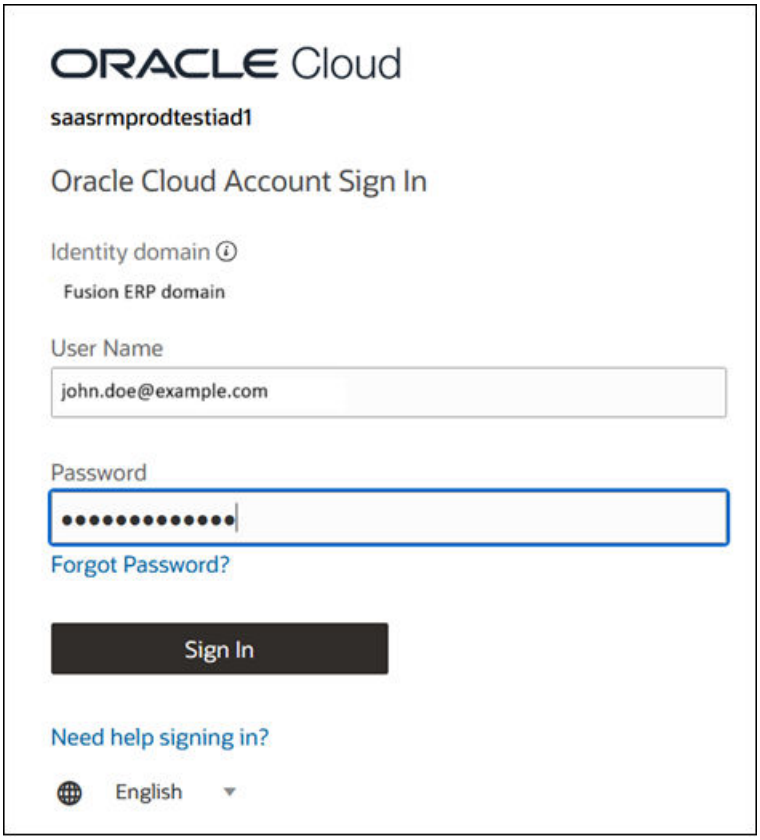
Start by signing in to the Oracle Cloud Console for each identity domain using two separate browser sessions. For example, if you are using Google Chrome, you can open one session in regular mode and the other in incognito mode. This allows you to have both consoles open at the same time, one for the source domain and other for the target domain.

The steps below guide you through signing in to the source domain. You can repeat them in a separate browser to sign in to the target domain.

1. Use the **Sign in with an identity domain** option to access each domain individually.

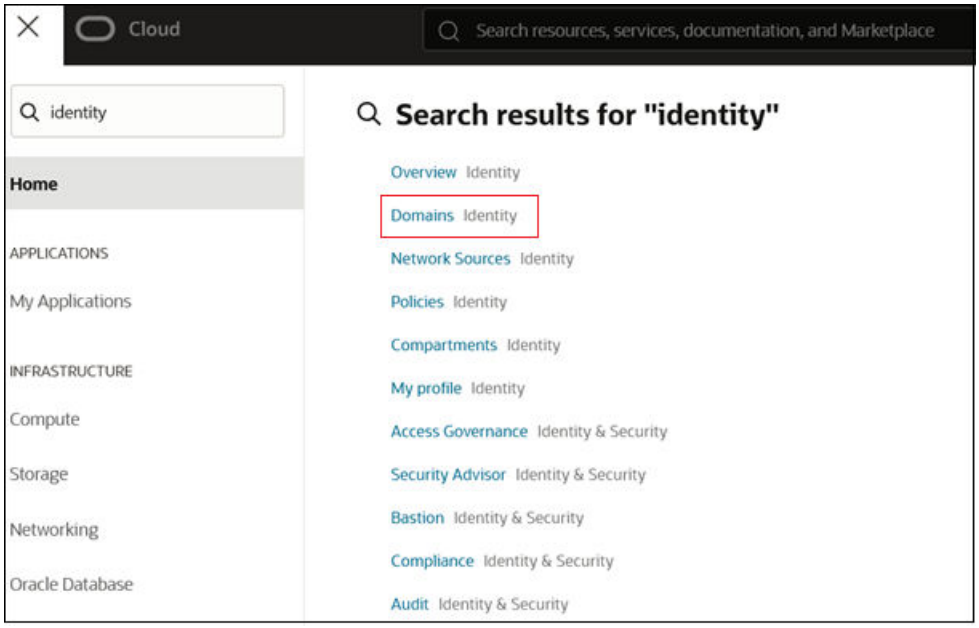


2. Enter your credentials in the domain. You may use Multi-factor authentication methods to sign in to the console. See Enabling Multifactor Authentication.

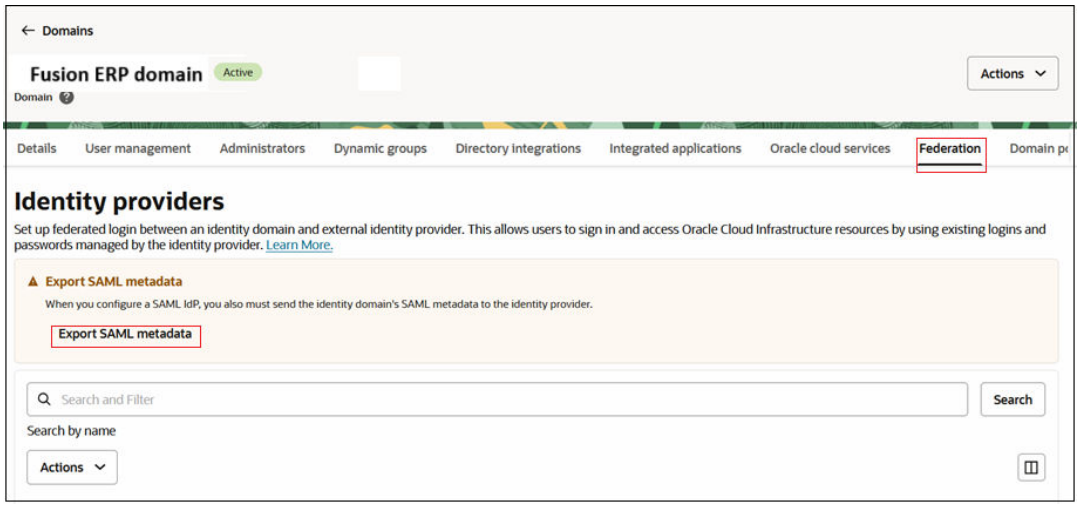


Step 2 - Fusion ERP Domain - Download Fusion ERP Metadata

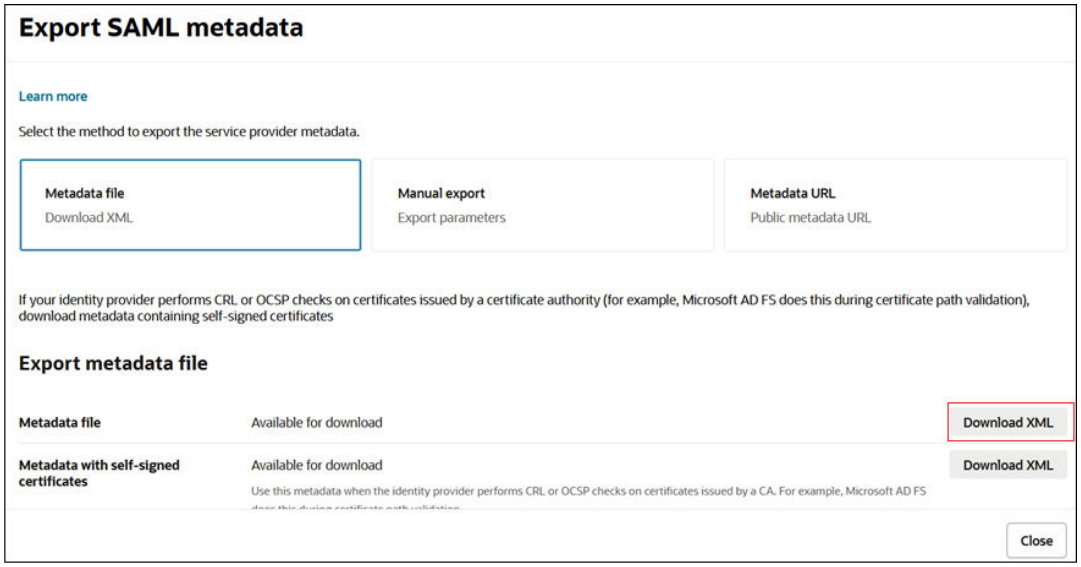
1. In the Fusion ERP domain, go to the **Navigation** menu, search for *Identity*, and select **Domains**.



2. Select the Fusion ERP domain to view the domain's details.
3. Navigate to the **Federation** tab.
4. Select **Export SAML metadata**.



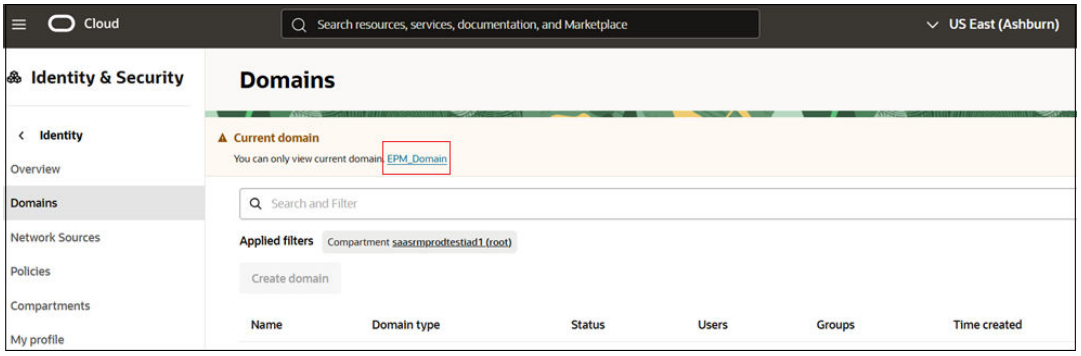
5. Download metadata file. You will use this file to configure Fusion ERP as an IdP in EPM domain.



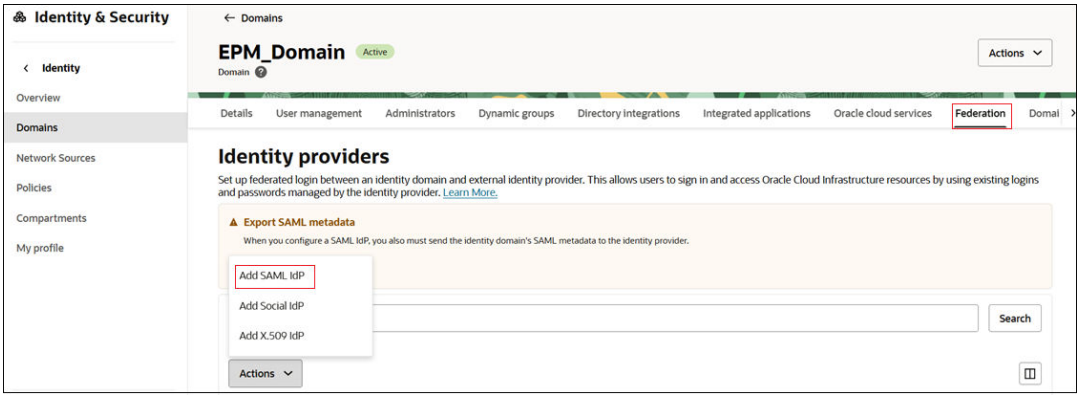
Step 3 - EPM Domain - Configure Fusion ERP as an Identity Provider

Configure the Fusion ERP service as a trusted identity provider in the Cloud EPM domain.

1. In the Cloud EPM domain, go to the **Navigation** menu, search for *Identity*, and select **Domains**.
2. Select the Cloud EPM domain to view the domain's details page.

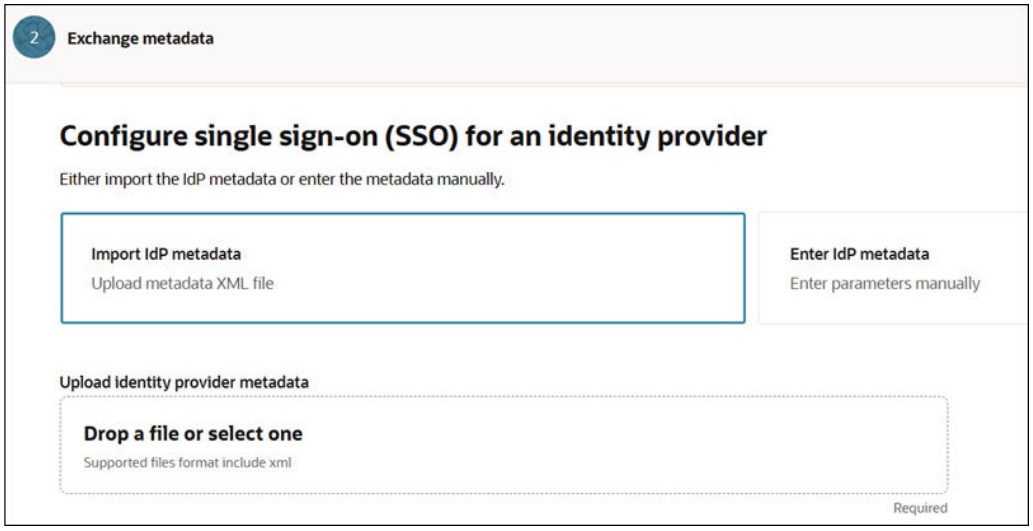


3. On the EPM Domain page, navigate to the **Federation** tab.
4. Click **Actions**, select **Add SAML IdP** and submit the tasks in the workflow.

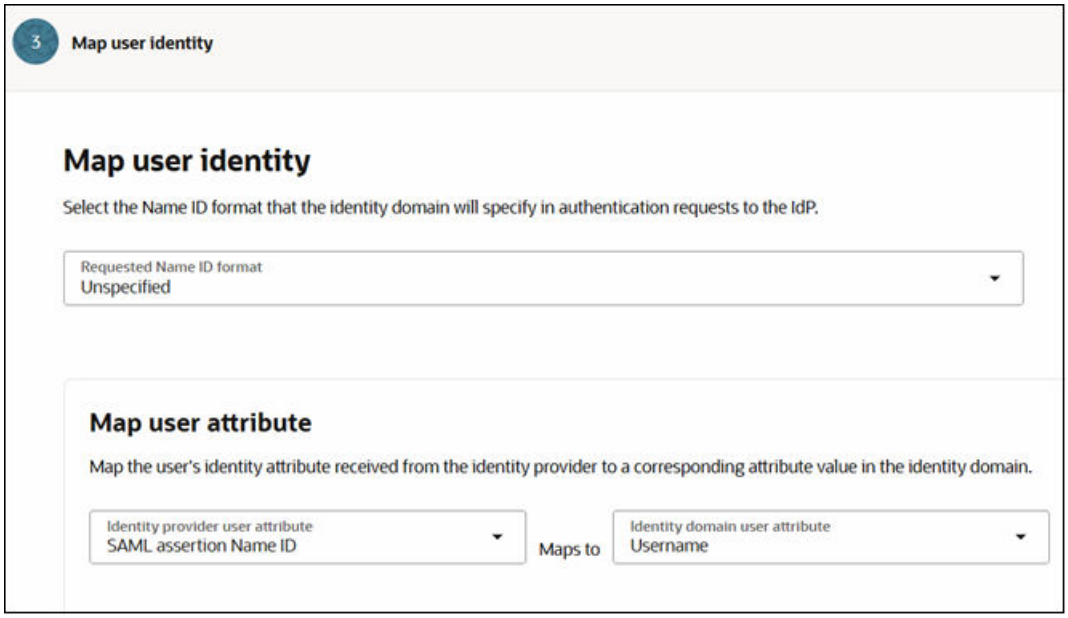


5. **Task 1 - Add details:**
   - **Name**: Enter the name of the SAML IdP.
   - (Optional) **Description**: Enter a description of the IdP.
   - (Optional) **Identity provider icon**: Drag and drop a supported image, or click **select one** to browse for the image.

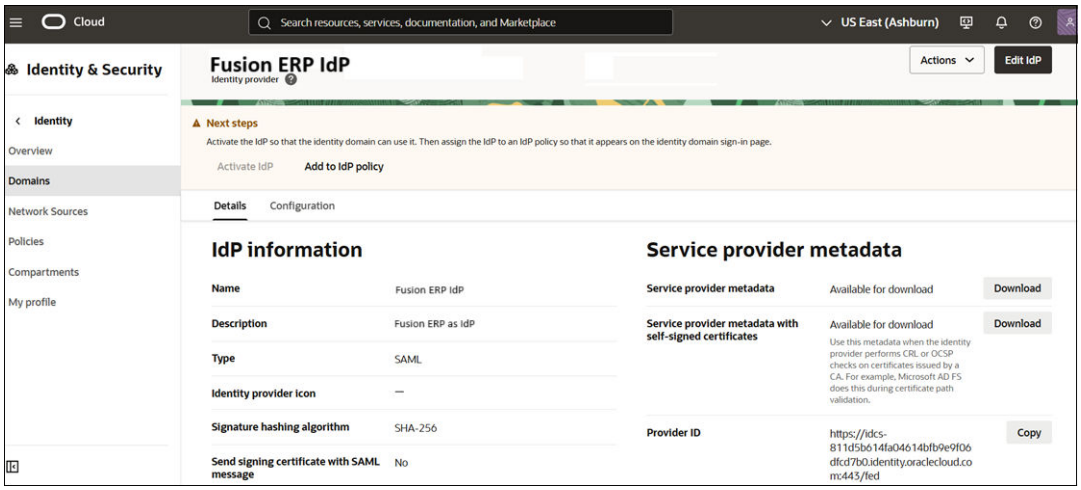
6. Click **Next**.
7. **Task 2 - Exchange metadata:**
   a. Select **Import IdP metadata**.
   b. Click **Drop a file or select one** to upload the metadata file you downloaded from Fusion ERP.



8. Click **Next**.
9. **Task 3- Map user identity**. Configure the fields as shown in referenced image:



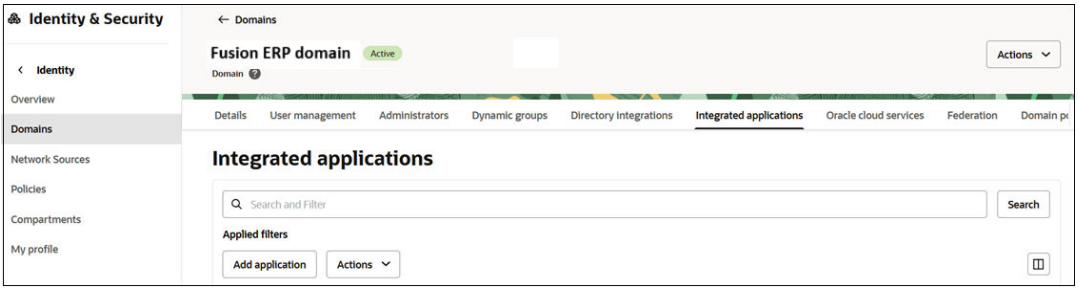
10. Click **Next**.
11. On the **Review and Create** page, verify the entered details. Click **Create IdP**.
    The Fusion ERP service gets listed under **Identity Providers** in the **Federation** tab.
12. Select Fusion ERP service identity provider you just created to open the **Details** page.



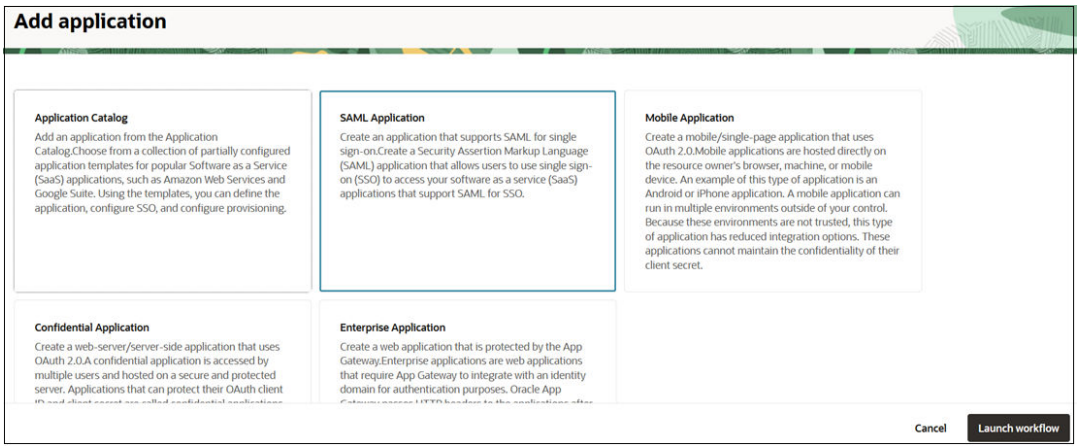
13. Click **Download** next to Service provider metadata.
14. Scroll down and click **Download** next to Service provider signing certificate.

Step 4 - Fusion ERP Domain - Add Cloud EPM as an Integrated Application

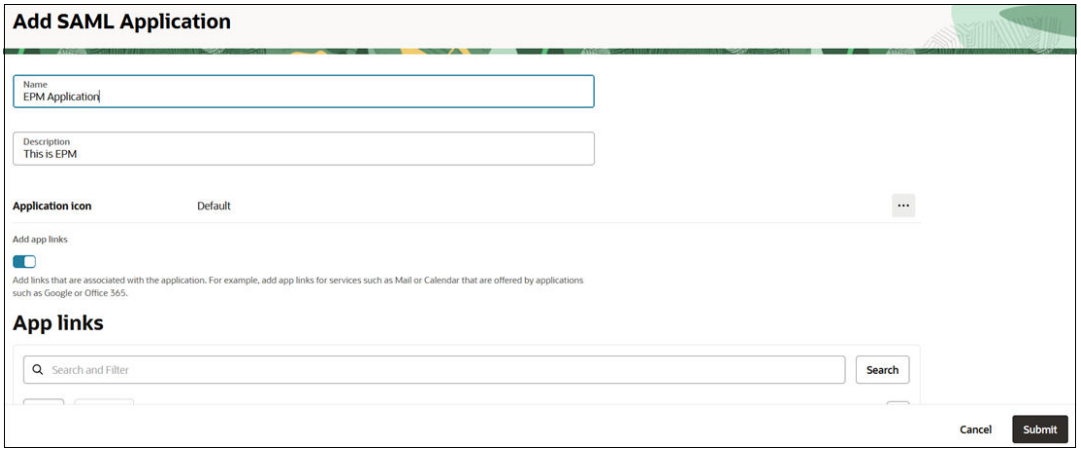
1. On the Fusion ERP Domain page, go to the **Integrated applications** tab.
2. Click **Add application**.



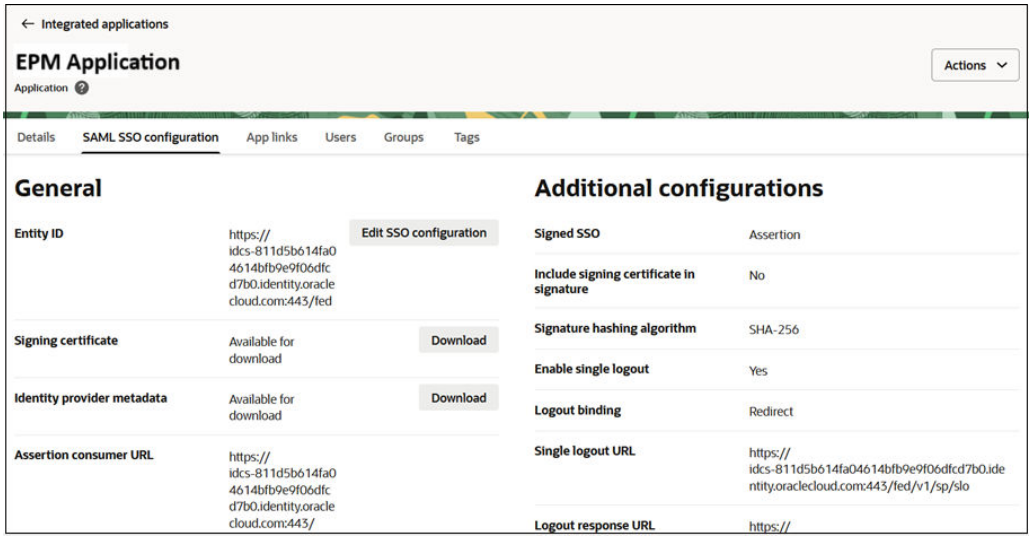
3. On the Add application page, select **SAML Application**.
4. Click **Launch workflow**.



5. Provide name and other details, and click **Submit**.



6. Configure SSO.
   a. Navigate to **SAML SSO configuration** tab.
   b. Click **Edit SSO configuration**.



c. Under **General**, enter the Service Provider metadata values that you downloaded in last section. See Step 3 - EPM Domain - Configure Fusion ERP as an Identity Provider. Map the fields as follows:

- **Entity ID** - *Provider ID*
- **Assertion consumer URL** - *Assertion Consumer Service URL*
- **Single logout URL** - *Logout Service Endpoint URL*
- **Logout respone URL** - *Logout response URL*

d. Configure additional SSO settings:

- **Name ID Format**: Select **Unspecified**
- **Name ID Value**: Select **Username**
- **Signing Certificate**: Upload the Service Provider signing certificate downloaded from the **Service Provider Metadata** screen. See Step 3 - EPM Domain - Configure Fusion ERP as an Identity Provider.

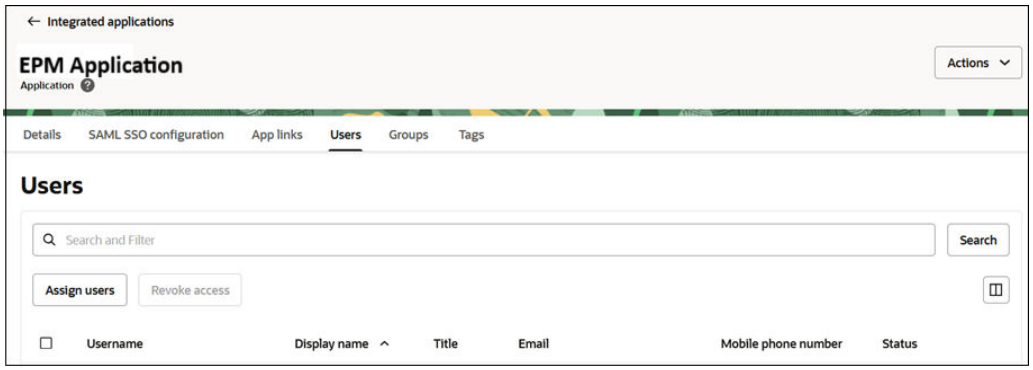
e. Click **Save changes**.

7. Assign users to the application.

a. Navigate to the **Users** tab.

b. Click **Action** on top, and then select **Activate** from the menu.

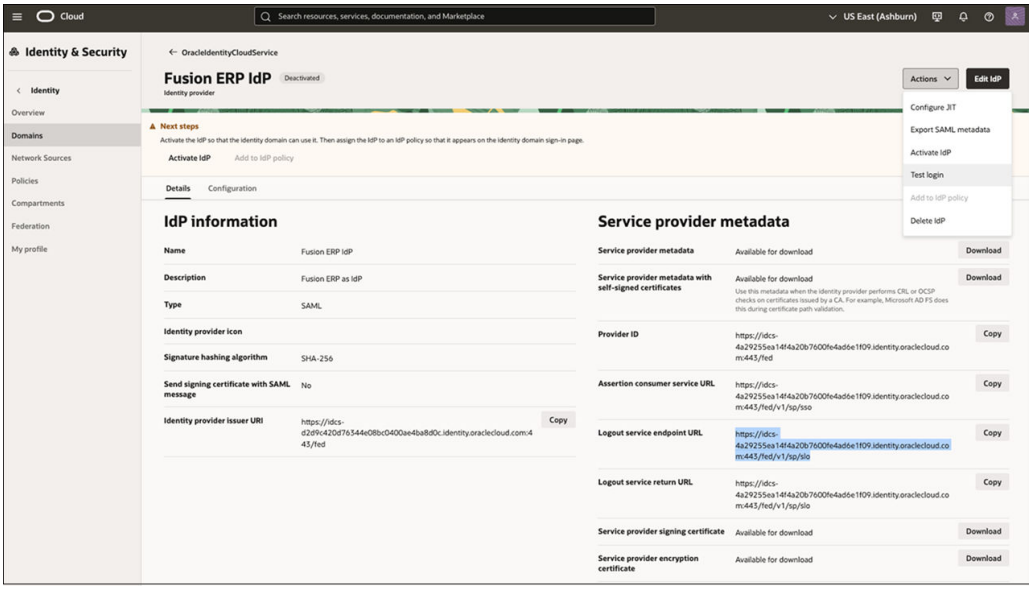
c. Next, click **Assign users**.



d. Search for and select users to assign this application to, and click **Assign**.

Step 5 - EPM Domain - Verify SAML SSO

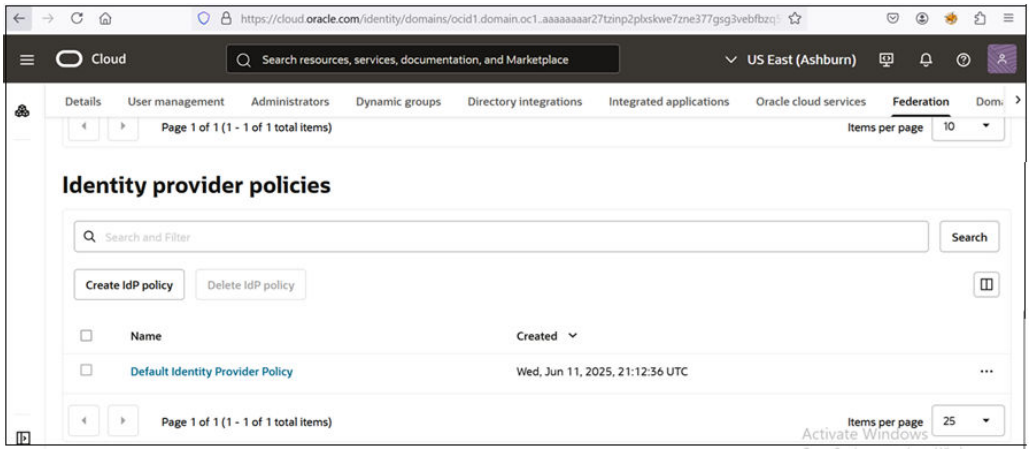
1. On the EPM Domain page, verify SAML SSO with your identity provider.
   a. Click **Actions** on top, and then select **Test login** from the menu.



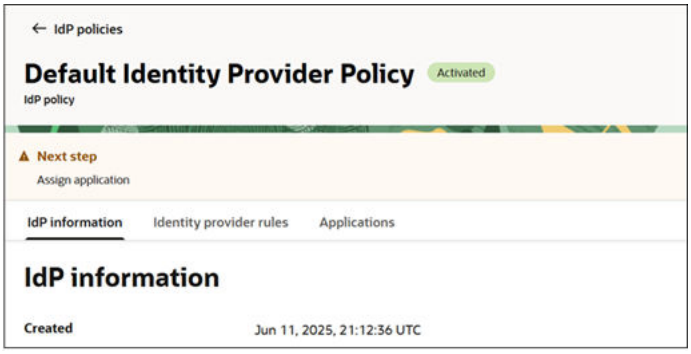
   b. Authenticate with your credentials to test the connection.
   If successful, a message will appear: **"Your connection is successful."**

2. Activate the Identity provider so that the identity domain can use it. Click **Actions**, then select **Activate IdP** from the menu.

3. Next, assign the identity provider to an IdP policy so that it appears on the identity domain sign-in page.
   a. Click **Actions**, and then select **Add to IdP Policy** from the menu.
   b. Scroll-down, under **Identity Provider Policies**, select the policy to assign.



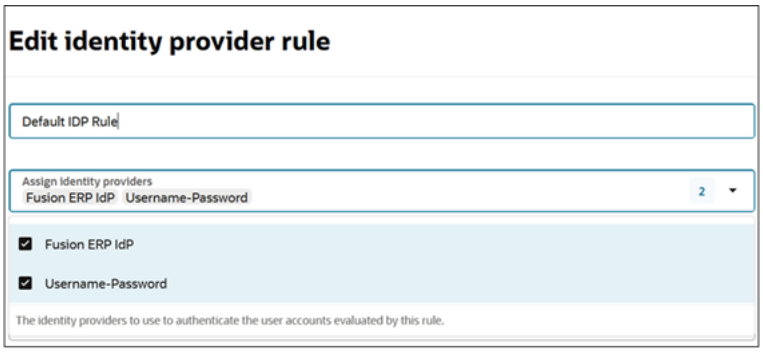
   c. Click on Default Identity Provider Policy.



d. Navigate to **Identity provider rules** tab.

e. Click the **ellipses** next to the IdP rule, then click select **Edit IdP rule.**

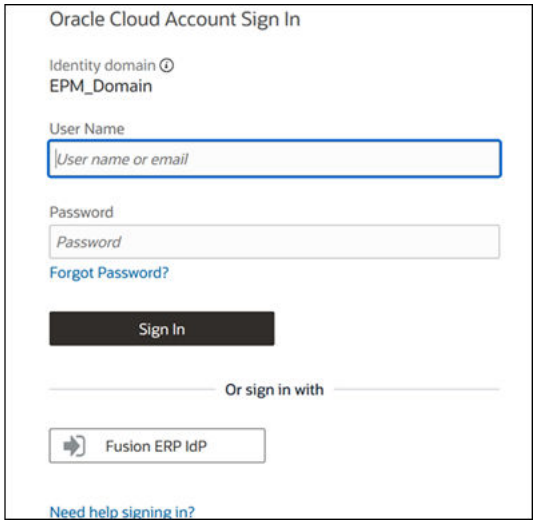
f. On the **Edit identity provider rule** page, in the **Assign identity providers** dropdown, select **Fusion ERP IdP** and **Username-Password**.



g. Click **Save changes**.

4. Click Profile icon on top and select **Sign out**.

5. Navigate to the Sign into the Console page in the EPM Domain. The **Fusion ERP IdP** button is displayed at the bottom.



Step 6 - Fusion ERP Domain - Test SSO

1. Login to Fusion ERP Domain.
2. In a separate browser window, navigate to the Cloud EPM Environment URL.
3. When prompted for authentication, select the SSO (Single Sign-On) provider.

   You will be automatically logged in to the Cloud EPM Environment without needing to re-enter your credentials.

Configuring SSO Between Services Across Different Cloud Accounts

You might have services deployed across two different cloud accounts. To provide a seamless user experience, you can configure Single Sign-On (SSO) between them.

Example Scenario

You have a user who needs to access both Oracle Fusion Cloud Enterprise Performance Management and Fusion ERP services, but these services are spread across two different Oracle Cloud accounts. Although the user exists in both accounts, to provide a seamless sign-on experience, you plan to set up SSO between these environments.

- Fusion ERP serves as the Identity Provider
- Cloud EPM functions as the Service Provider

In this topic, we'll walk through how to configure SSO for this scenario:

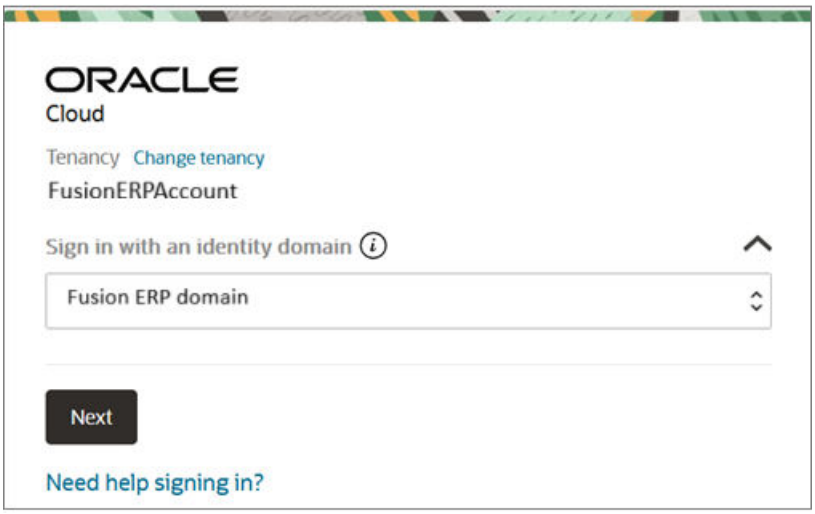
- Step 1 - Open Separate Sessions for Each Cloud Account
- Step 2 - Fusion ERP Cloud Account - Download Fusion ERP Metadata
- Step 3 - Cloud EPM Account - Configure Fusion ERP as an Identity Provider
- Step 4 - Fusion ERP Cloud Account - Add Cloud EPM as an Integrated Application
- Step 5 - Cloud EPM Account - Verify SAML SSO
- Step 6 - Test SSO

Step 1 - Open Separate Sessions for Each Cloud Account

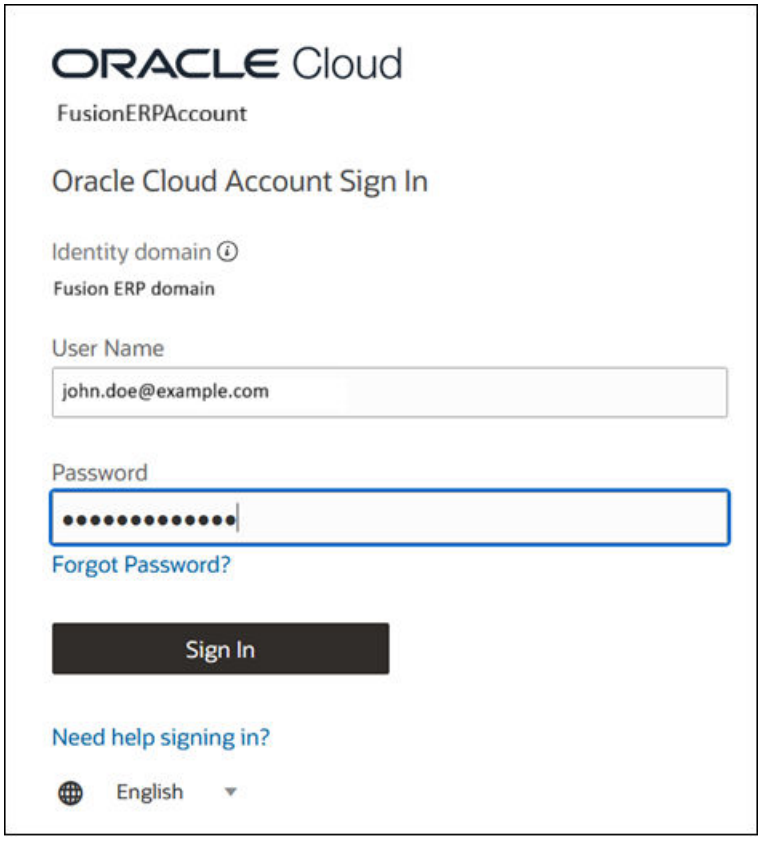
Sign-in to the Oracle Cloud Console for each of your subscribed cloud accounts.

The following example is to sign in to Fusion ERP cloud account. Follow the same steps to open the Cloud EPM account as well.

1. On the sign-in page, select **Sign in with an Identity Domain**. Ensure your tenancy and domain name are correct. Click **Next**.



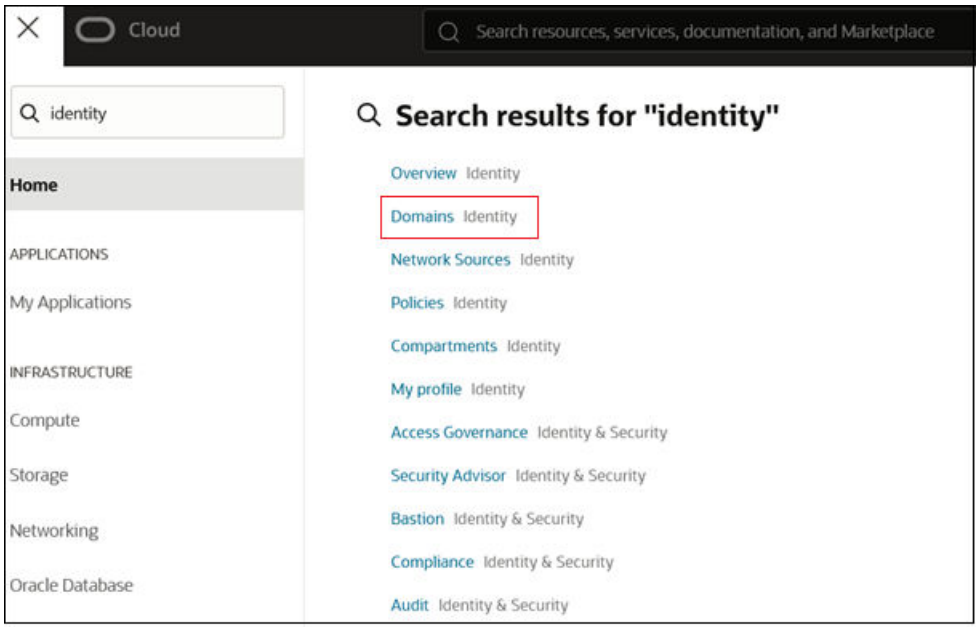
2. Sign in using your credentials. Multi-factor authentication (MFA) may be required to access the console. See Enabling Multifactor Authentication.



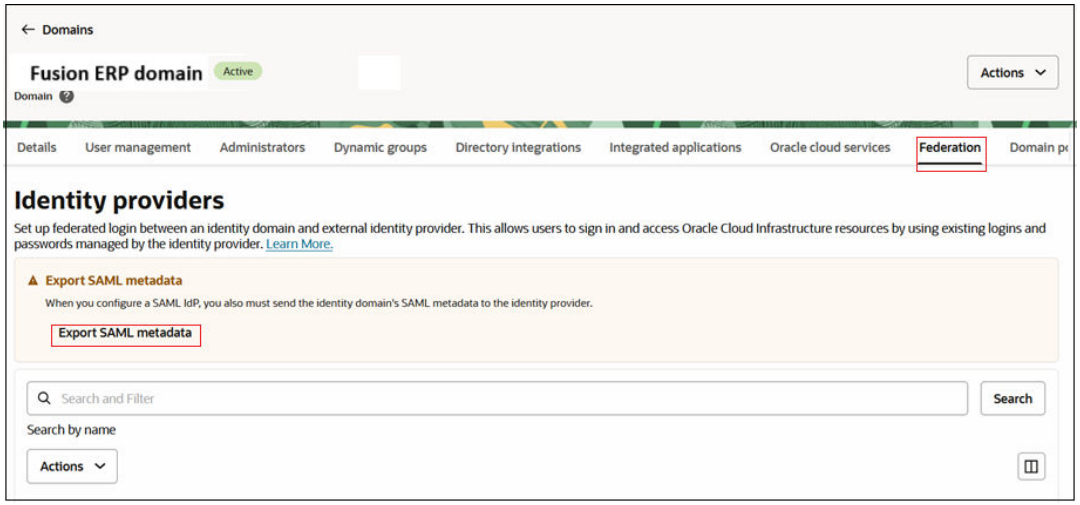
After successful authentication, the Oracle Cloud Console opens.

Step 2 - Fusion ERP Cloud Account - Download Fusion ERP Metadata

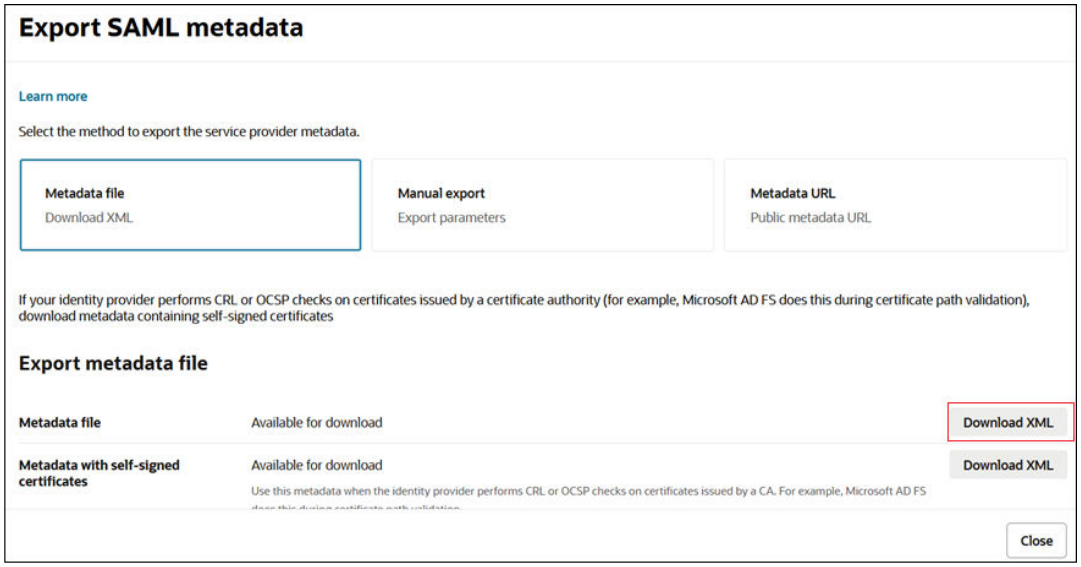
1. In the Fusion ERP cloud account, go to the **Navigation** menu, search for *Identity*, and select **Domains**.



2. Select the Fusion ERP domain to view the domain's details.
3. Navigate to the **Federation** tab.
4. Select **Export SAML metadata**.



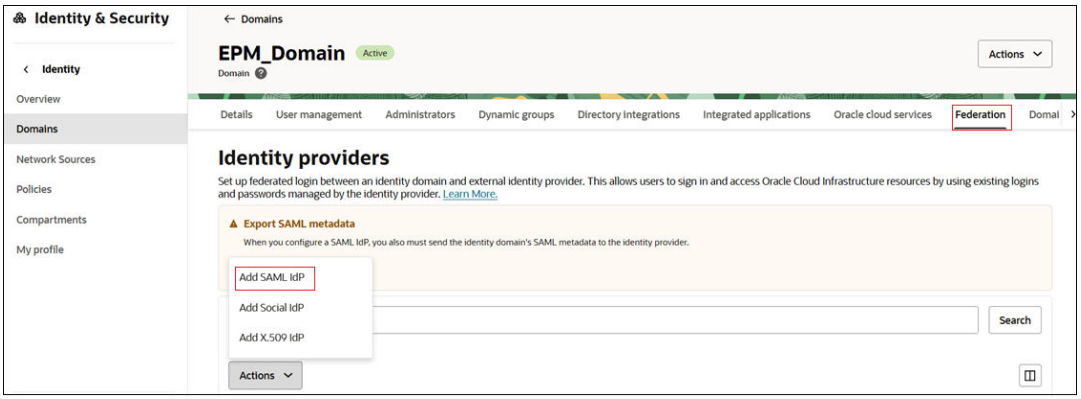
5. Download metadata file. You will use this file to configure Fusion ERP as an IdP in EPM cloud account.



Step 3 - Cloud EPM Account - Configure Fusion ERP as an Identity Provider

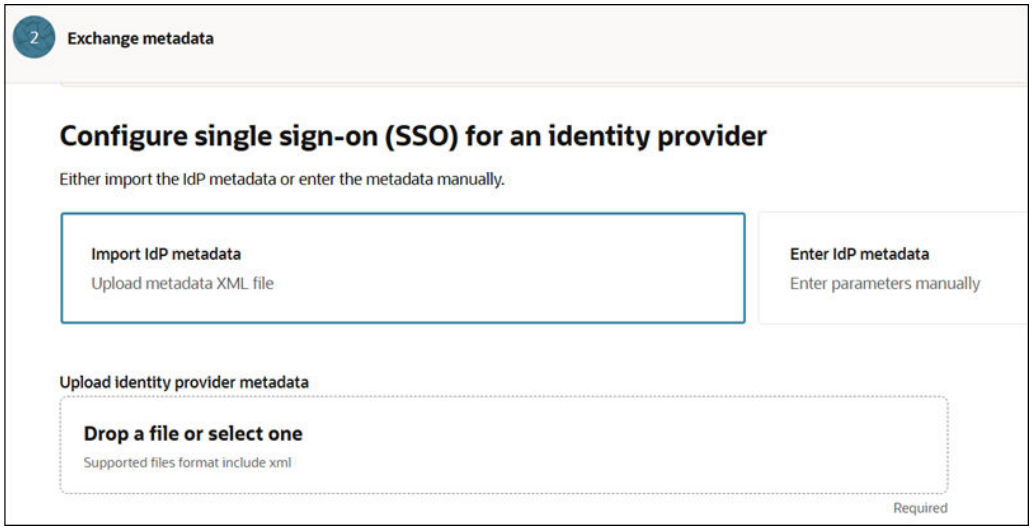
Configure the Fusion ERP service as a trusted identity provider in the Cloud EPM account.

1. In the Cloud EPM account, go to the **Navigation** menu, search for *Identity*, and select **Domains**.
2. Select the Cloud EPM domain to view the domain's details page.
3. Navigate to the **Federation** tab.
4. Click **Actions**, select **Add SAML IdP** and submit the tasks in the workflow.

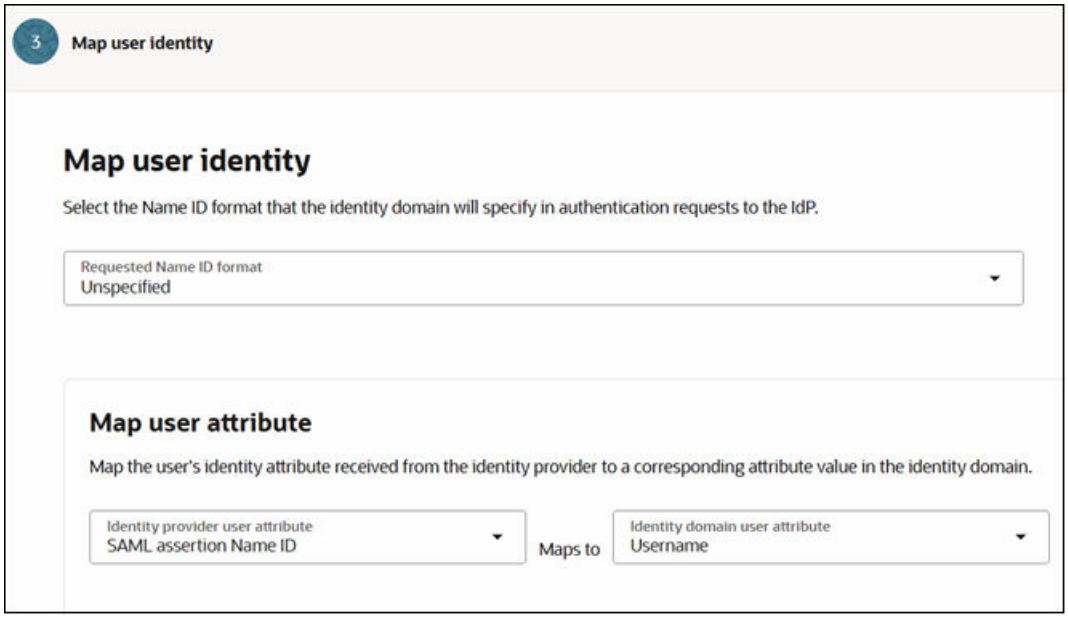


5. **Task 1 - Add details:**
   - **Name**: Enter the name of the SAML IdP.
   - (Optional) **Description**: Enter a description of the IdP.
   - (Optional) **Identity provider icon**: Drag and drop a supported image, or click **select one** to browse for the image.

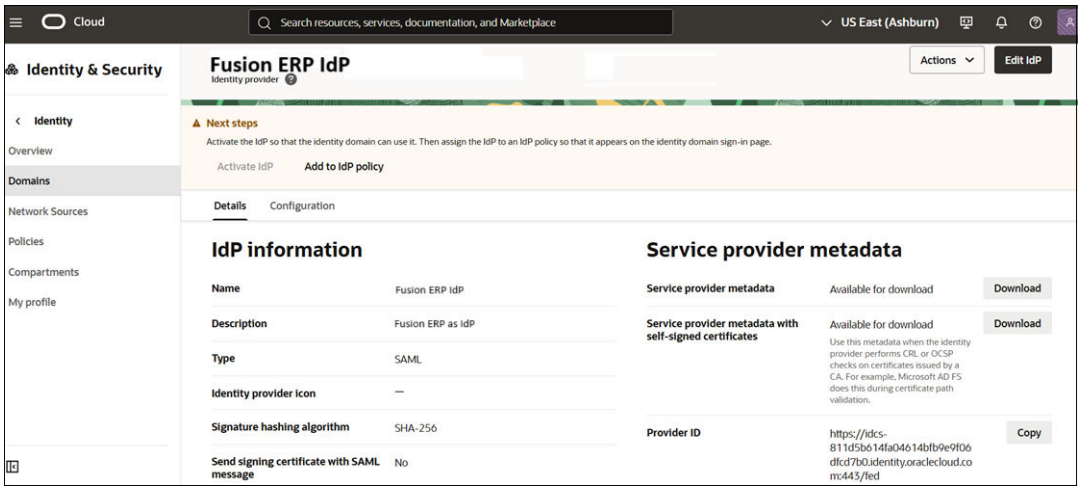
6. Click **Next**.
7. **Task 2 - Exchange metadata:**
   a. Select **Import IdP metadata**.
   b. Click **Drop a file or select one** to upload the metadata file you downloaded from Fusion ERP. See Step 2 - Fusion ERP Cloud Account - Download Fusion ERP Metadata



8. Click **Next**.
9. **Task 3- Map user identity**. Configure the fields as shown in referenced image:



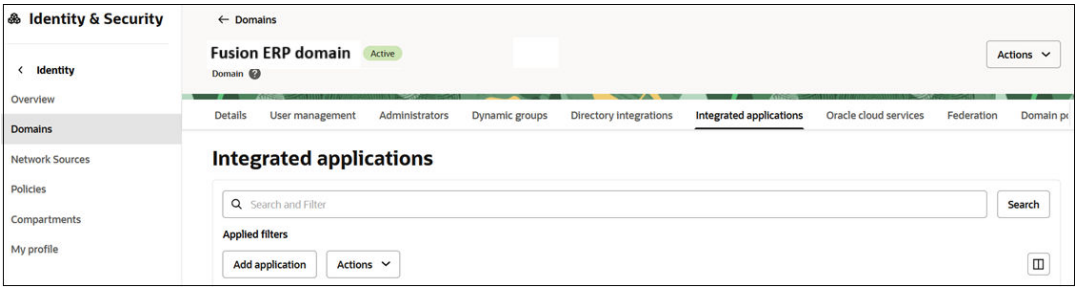
10. Click **Next**.
11. On the **Review and Create** page, verify the entered details. Click **Create IdP**.
    The Fusion ERP service gets listed under **Identity Providers** in the **Federation** tab.
12. Select Fusion ERP service identity provider you just created to open the **Details** page.



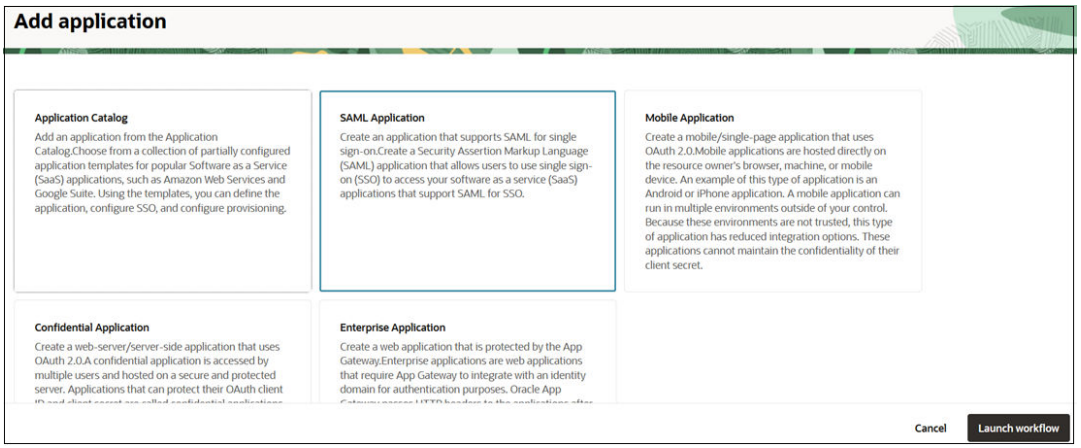
13. Click **Download** next to Service provider metadata.
14. Scroll down and click **Download** next to Service provider signing certificate.

Step 4 - Fusion ERP Cloud Account - Add Cloud EPM as an Integrated Application

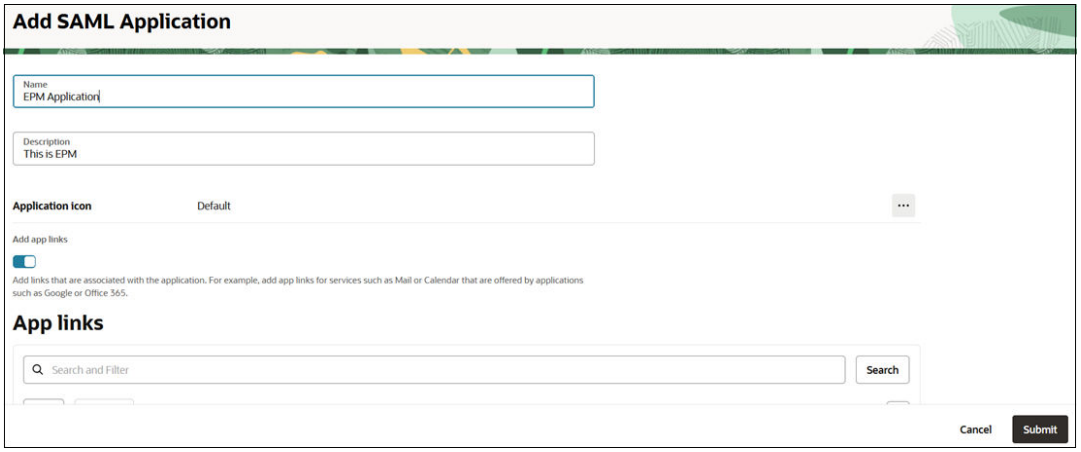
1. Go to the **Integrated applications** tab.
2. Click **Add application**.



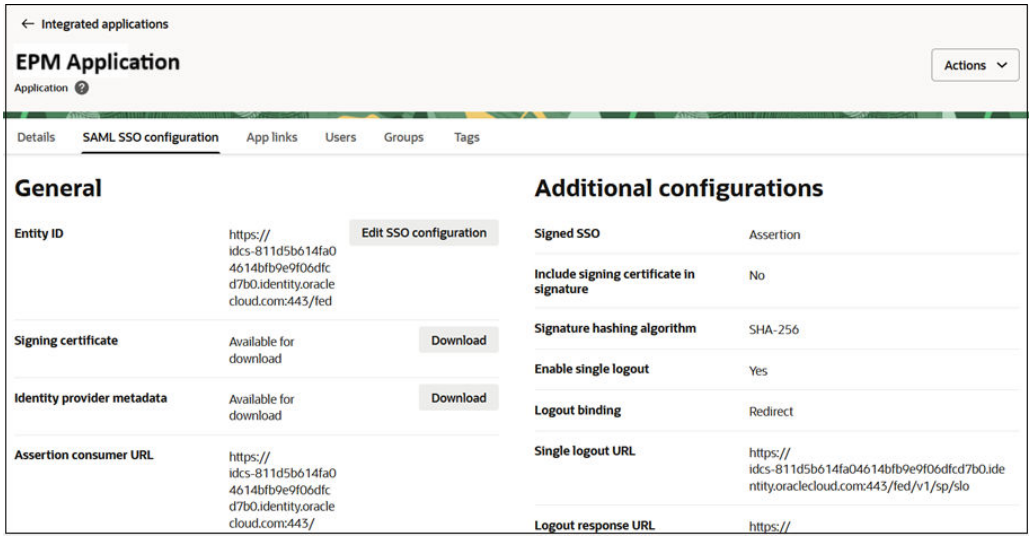
3. On the Add application page, select **SAML Application**.
4. Click **Launch workflow**.



5. Provide name and other details, and click **Submit**.



6. Configure SSO.
   a. Navigate to **SAML SSO configuration** tab.
   b. Click **Edit SSO configuration**.



c. Under **General**, enter the Service Provider metadata values that you downloaded in last section. See Step 3 - Cloud EPM Account - Configure Fusion ERP as an Identity Provider . Map the fields as follows:

- **Entity ID** - *Provider ID*
- **Assertion consumer URL** - *Assertion Consumer Service URL*
- **Single logout URL** - *Logout Service Endpoint URL*
- **Logout respone URL** - *Logout response URL*

d. Configure additional SSO settings:

- **Name ID Format**: Select **Unspecified**
- **Name ID Value**: Select **Username**
- **Signing Certificate**: Upload the Service Provider signing certificate downloaded from the **Service Provider Metadata** screen. See Step 3 - Cloud EPM Account - Configure Fusion ERP as an Identity Provider.

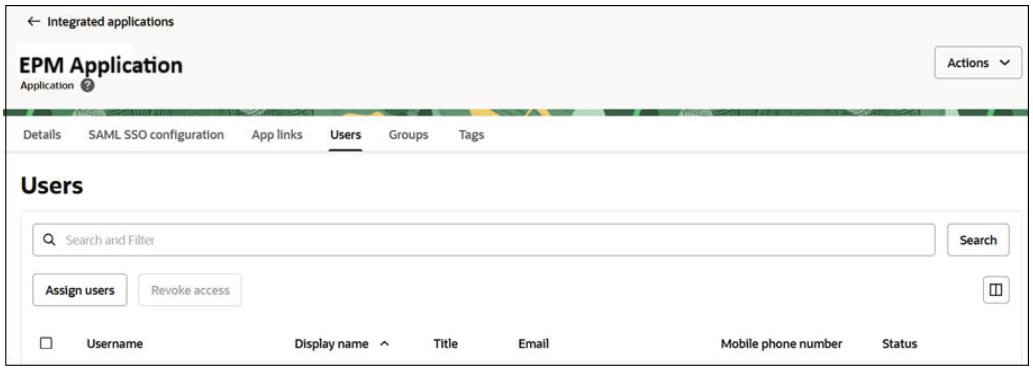
e. Click **Save changes**.

7. Assign users to the application.

a. Navigate to the **Users** tab.

b. Click **Action** on top, and then select **Activate** from the menu.

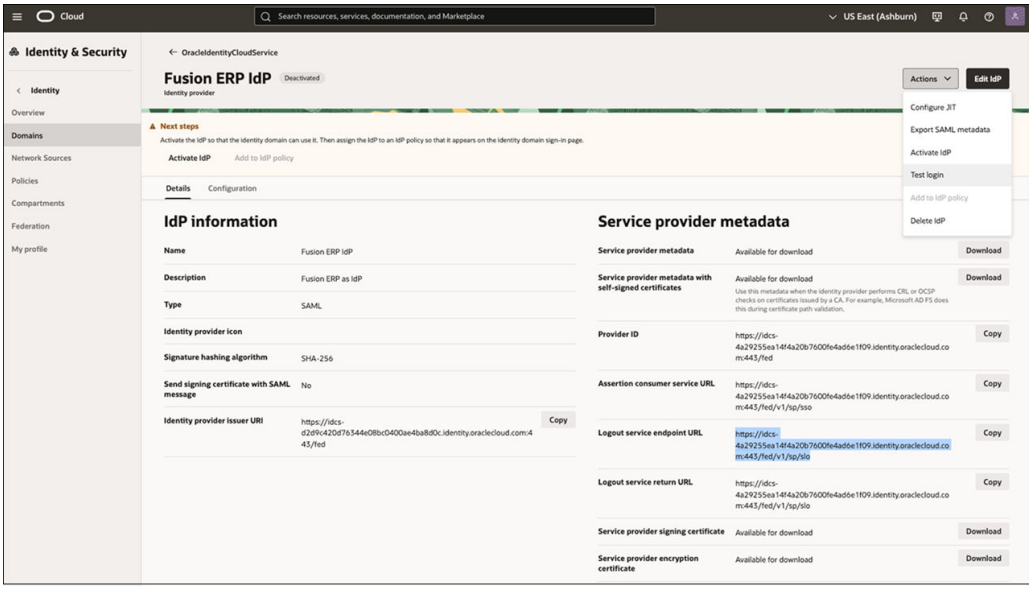
c. Next, click **Assign users**.



d. Search for and select users to assign this application to, and click **Assign**.

Step 5 - Cloud EPM Account - Verify SAML SSO

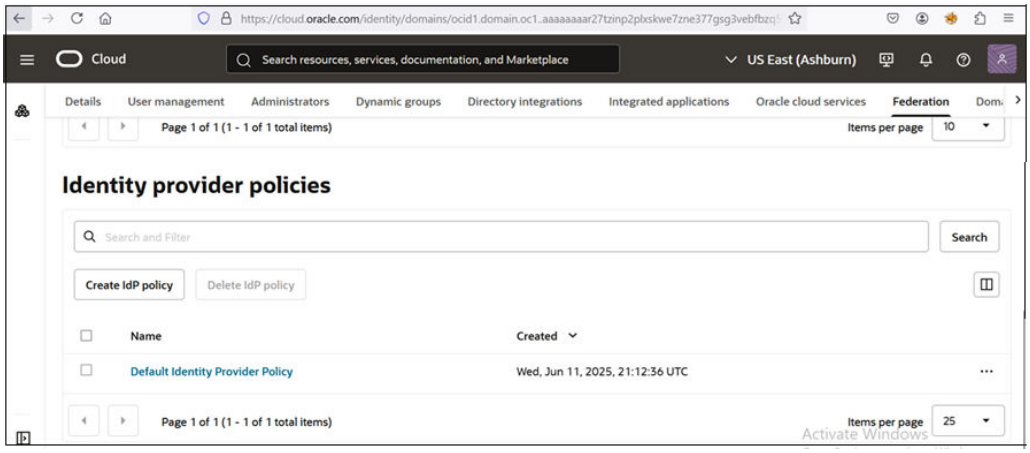
1. Verify SAML SSO with your identity provider.
   a. Click **Actions** on top, and then select **Test login** from the menu.



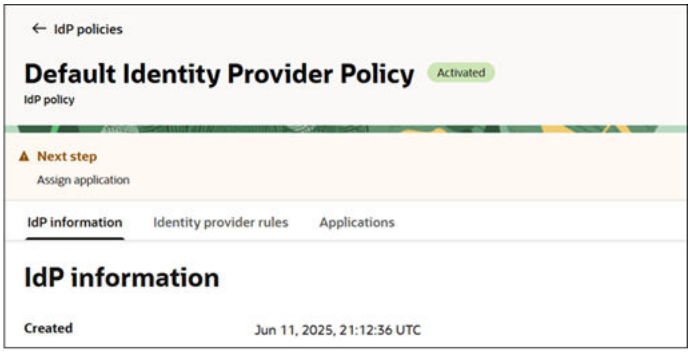
   b. Authenticate with your credentials to test the connection.
   If successful, a message will appear: **"Your connection is successful."**

2. Activate the Identity provider so that the identity domain can use it. Click **Actions**, then select **Activate IdP** from the menu.

3. Next, assign the identity provider to an IdP policy so that it appears on the identity domain sign-in page.
   a. Click **Actions**, and then select **Add to IdP Policy** from the menu.
   b. Scroll-down, under **Identity Provider Policies**, select the policy to assign.



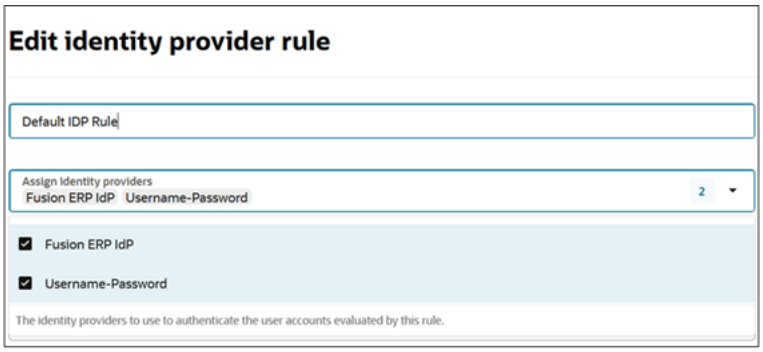
   c. Click on Default Identity Provider Policy.



d. Navigate to **Identity provider rules** tab.

e. Click the **ellipses** next to the IdP rule, then click select **Edit IdP rule.**

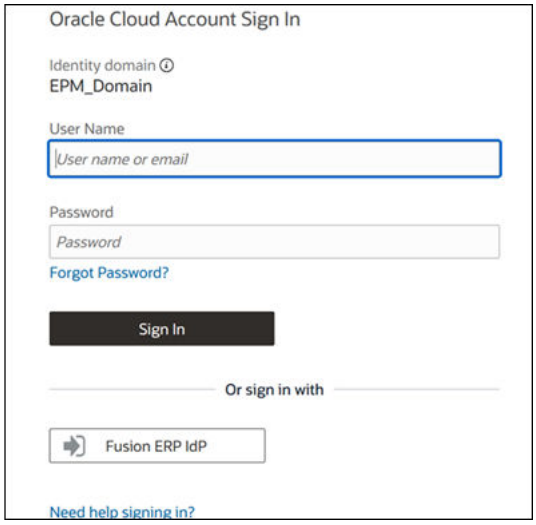
f. On the **Edit identity provider rule** page, in the **Assign identity providers** dropdown, select **Fusion ERP IdP** and **Username-Password**.



g. Click **Save changes**.

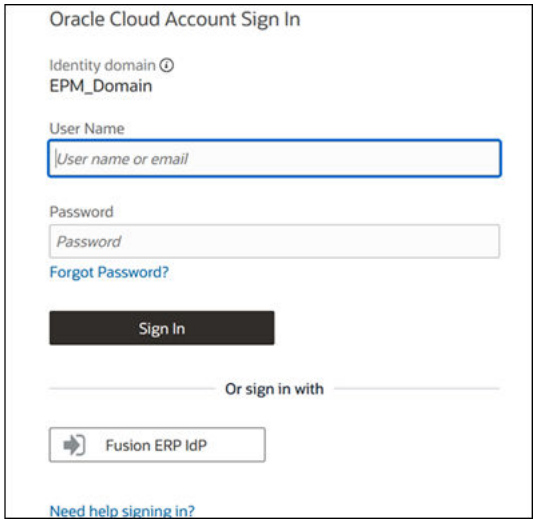
4. Click Profile icon on top and select **Sign out**.

5. Sign in again to the Cloud EPM account. The **Fusion ERP IdP** button is displayed at the bottom.



Step 6 - Test SSO

1. Sign out of both your Fusion ERP and Cloud EPM accounts, then close your browsers.
2. First, sign to your Fusion ERP cloud account.
3. Next, open your Cloud EPM URL in a separate tab.



4. On the Cloud EPM sign-in page, click **Fusion ERP IdP**.
   You will be automatically authenticated and redirected to the Cloud EPM environment without re-entering your credentials.

Successful sign-in through the Fusion ERP IdP confirms that SSO is configured between your Fusion ERP and Cloud EPM accounts.

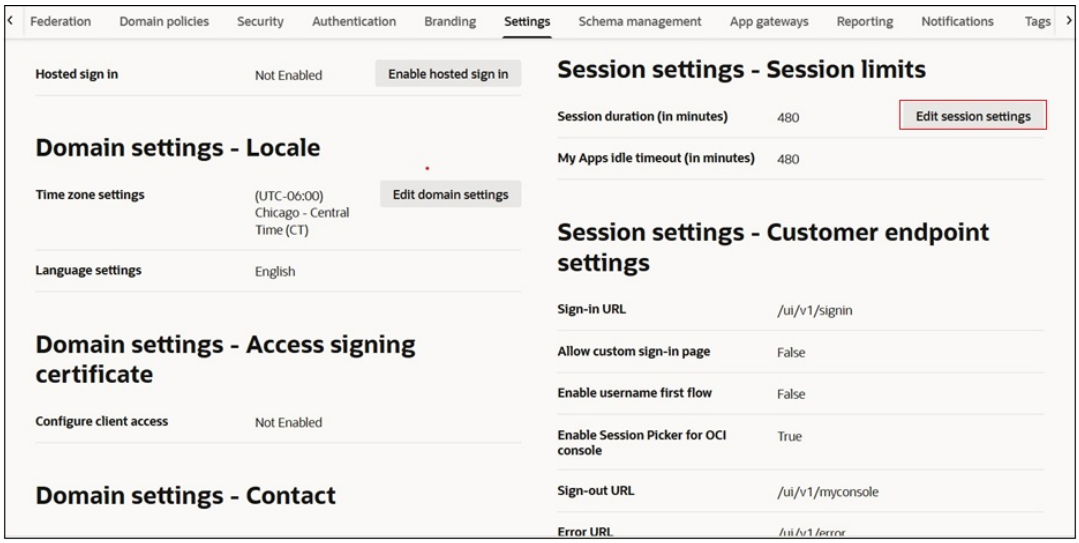
Customizing Logout URL for SSO-Enabled Cloud EPM and Cloud EDM Environments

The logout URL of Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments is, by default, set to revert to your

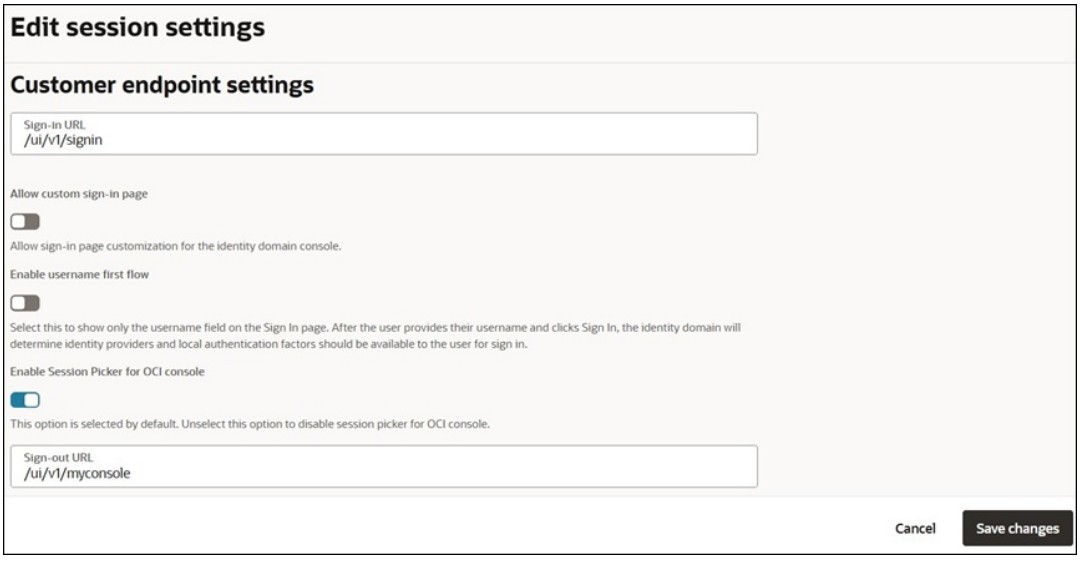
login page. You can change the logout page, especially in SSO-enabled environments, so that a custom page of your choice (usually an identity provider (IdP) page) is displayed when you sign out. The custom logout page you specify is maintained even if you recreate your environment.

To display a page of your choice on logging out of an environment:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. Navigate to **Settings** tab.
3. Scroll down to **Session settings - Session limits**.
4. Click **Edit session settings**.



5. On Edit session settings page, enter **Sign-out URL** of the page you want displayed.



6. Click **Save changes**.
   The new sign-out URL will take effect after the next daily maintenance. See Managing Daily Maintenance.

Managing User Credentials for SSO-Enabled Cloud EPM and Cloud EDM Environments

Once you have enabled Single Sign-On (SSO) in your environments, you get two sign-in options — Company Sign-In (SSO) and Traditional Cloud Account Sign-In.

However, some client components do not work with SSO credentials; for example:

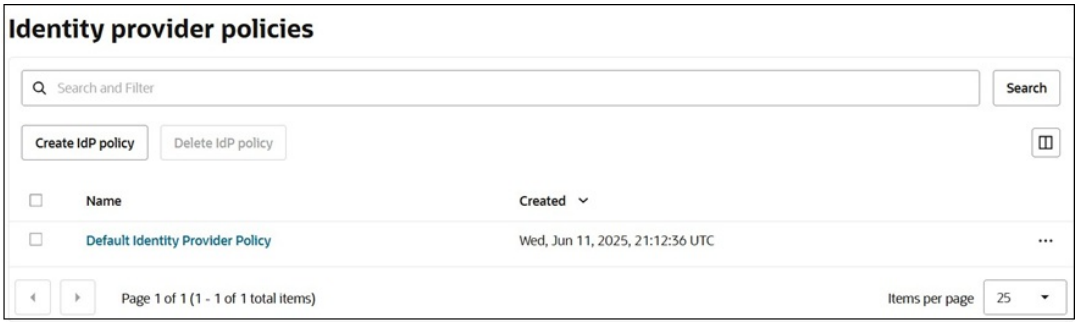
- The basic authentication used by EPM Agent and EPM Automate does not work with the SSO credentials.
- Cross-environment connections do not work with the SSO credentials of the Service Administrator.

In these scenarios, it is crucial to ensure that these users maintain their identity domain credentials. Additionally, you may also want the users to not be able to login with Traditional Cloud Account Sign-In and only login using SSO login.

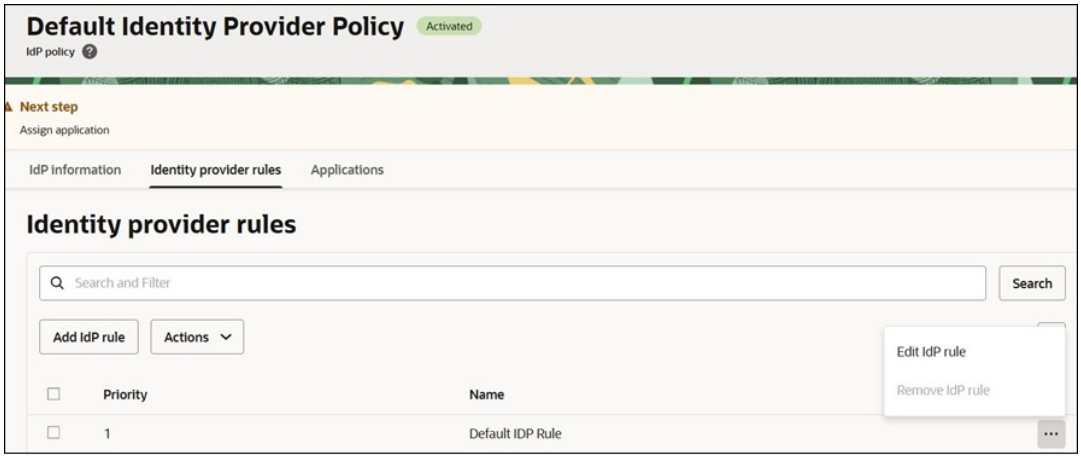
Here are the instructions on how you can ensure that appropriate users are allowed to login using SSO credentials and/or identity domain credentials:

The SSO-enabled Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments automatically maintain the identity domain credentials. By default, when the users use a browser to access an environment, they see both sign-in options. If you want the browser users to not see the Traditional Cloud Account Sign In option and login only using SSO, do the following:

1. Sign into IAM Interface as an Identity Domain Administrator. See Accessing the IAM Interface.
2. On the **Federations** tab, scroll-down to **Identity providers policies**.
3. Click the default IdP policy.



4. To view IdPs assigned to the policy, navigate to **Identity provider rules** tab.
5. Click **Ellipses ...** next to the IdP policy rule, and then and select **Edit IdP rule** from the menu.



6. Remove **Username-Password** from the **Assign identity providers** box.
7. Click **Save changes**.

Avoiding Password Expiry Emails

When the credentials of the users are stored in identity domain, they get password expiry emails when those passwords are expired. If you have setup SSO with an IdP after these users are created and you don't want the credentials for these users to be stored in the identity domain and for them to not get password expiry emails, you must delete these users and recreate them after enabling SSO.

Making Smart View (Mac and Browser) Work after Enabling SSO

After you set up SSO with an identity provider (IdP), Oracle Smart View for Office (Mac and Browser) will not work until you complete these tasks:

- Create a new manifest file with the domain of the IdP
- Redeploy the manifest file

For detailed information, see these topics in *Deploying and Administering Oracle Smart View for Office (Mac and Browser)* :

- Creating and Saving the Manifest File
- Deploying the Manifest File to Office 365 Users

Troubleshooting

See Fixing Smart View Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Setting up Network Perimeter

You can set up a Network Perimeter in Oracle Identity Cloud Service to limit sign-ins to users from specific IP addresses or ranges. This method allows you to control access to all Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments within a designated identity domain.

See Manage Oracle Identity Cloud Service Network Perimeters in *Administering Oracle Identity Cloud Service*.

Deprecated Feature: Setting up Secure Access for Cloud EPM and Cloud EDM

The EPM Automate commands `getIPAllowlist` and `setIPAllowlist` could be used to create and manage an IP allowlist for your Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. For more details, refer to the descriptions of these commands in *Working with EPM Automate* guide:

- getIPAllowlist
- setIPAllowlist

> **Note**
>
> This functionality is now deprecated. You should use Network Perimeter instead. For more information, see Setting up Network Perimeter.

Troubleshooting

See Resolving IP Allowlist Functional Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Migrating from Per-Environment IP Allowlist to Network Perimeter in an Identity Domain

Currently, you can set the IP allowlist for a particular environment using `setIPAllowlist` EPM Automate command. Alternatively, IP allowlists for an entire identity domain can be configured using **Network Perimeter** settings in Identity Cloud Service. See Setting up Network Perimeter.

However, the per-environment IP allowlist functionality is deprecated and will be removed in the future. Once deprecated, any IP restrictions set using `setIPAllowlist` will no longer apply and your environment will begin accepting requests from all IP addresses by default.

To maintain your security posture and ensure continuity, you must migrate all IP allowlists defined per environment to the Network Perimeter of the corresponding identity domain. Here's how:

1. If you have multiple environments within an identity domain, use the `getIPAllowlist` EPM Automate command on each environment to retrieve their configured IP addresses and CIDRs.
2. Combine all these IP addresses and CIDRs into a single consolidated list.
3. Add the unique, non-overlapping entries from that list into the **Network Perimeter** settings of the identity domain in Oracle Cloud Console.

This ensures your IP-based access controls remain in place after the deprecation takes effect.

Restricting Access to Cloud EPM and Cloud EDM Environments Using Sign-On Policies

The default sign-on policy in Oracle Identity Cloud Service allows all users assigned to predefined roles to sign-in to an environment by supplying their credentials (user name and password). Identity Domain Administrators may configure a custom sign-on policy to determine whether a user is allowed to access Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. For example, you may configure a policy that allows only users assigned to the Service Administrator role to access the environments.

If you configure a custom sign-on policy, ensure that it allows all Cloud EPM users to sign in. For detailed information on setting sign-on policy, see these topics in *Administering Oracle Identity Cloud Service*:

- Understand Sign-On Policies
- Add a Sign-On Policy

Troubleshooting

See Troubleshooting Issues with Sign-On Policies in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Identifying and Deleting Unused Environments for Improved Security

Unused environments can pose potential security risks, as they may be targeted by malicious actors. Regularly deleting environments that are no longer in use helps reduce the attack surface and enhances overall security. In some cases, compliance requirements may also mandate the removal of inactive environments.

To identify and delete an unused environment:

1. Sign in to the environment and view the latest **Activity Report**. See Using the Activity Report.
2. In the **Number of Users** table, if all values are zero, it indicates the environment has been inactive for at least 30 days. See User Information.

Number of Users

Metric	05/15	05/16	05/17	05/18	05/19	05/20	Today
Average Duration (Hour:Min)	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Unique Users Count	0	0	0	0	0	0	0
Unique Users in Last 30 Days	0	0	0	0	0	0	0
Unique Users in Last 7 Days	0	0	0	0	0	0	0

3. If you decide to delete an environement, see Deleting an Environment.

> **Note**
>
> - You can delete a test or production environment individually. It's not necessary to delete both if only one is unused.
> - Deleting an environment permanently removes all data within it and invalidates its URLs. All its backups are also deleted 60 days after the deletion. If you don't plan to recreate the environment within 60 days, ensure you back up any important data and snapshots before proceeding.

Ensuring Task Manager Displays Oracle Cloud ERP Tasks

> **Note**
>
> This procedure applies to Financial Consolidation and Close, Tax Reporting, and those Planning applications where Task Manager is enabled.

To display the Oracle Cloud ERP tasks in Task Manager, you must allow the embedding of Oracle Cloud ERP URL within Oracle Fusion Cloud Enterprise Performance Management.

If you see a blank page with the error `Refused to connect <Oracle Cloud ERP URL>" when opening the Oracle Cloud ERP`", ensure that you complete the prerequisite procedure explained in End User Integrations for Oracle Cloud ERP in *Administering Financial Consolidation and Close* .

Accessing Compliance Reports

Oracle conducts regular third-party security assessments to ensure the effectiveness of its administrative and technical controls. The resulting compliance documentation includes:

- SOC 1 Report (based on SSAE No 18)
- SOC 2 Report
- Bridge Letter
- ISO Certificate
- Disaster Recovery Evidence Document
- Security Assessment Report

Who Can Access Compliance Reports?

By default, only Service Administrators can access compliance reports. To grant access to users without the Service Administrator role, add them to an IAM group and define the following policies for that group:

```
Allow group GROUP_NAME to {EPM_COMPLIANCEDOC_INSPECT, EPM_COMPLIANCEDOC_READ} in tenancy
```

```
Allow group GROUP_NAME to {EPM_PLANNING_COMPLIANCEDOC_INSPECT
EPM_PLANNING_COMPLIANCEDOC_READ} in tenancy
```

Example:

```
Allow group CompDocsGroup to {EPM_COMPLIANCEDOC_INSPECT, EPM_COMPLIANCEDOC_READ}
in tenancy
```

```
Allow group CompDocsGroup to
{EPM_PLANNING_COMPLIANCEDOC_INSPECT,EPM_PLANNING_COMPLIANCEDOC_READ} in tenancy
```

For more information, see Creating Policies for Users and Groups.

Downloading Compliance Reports

To download a compliance report:

1. Sign in to the Oracle Cloud Console.
2. Go to the **Navigation** menu, search for *Identity & Security*, and click **Compliance**. The **Compliance Documents** page displays all documents you have permission to view.
3. Find the document you want to download, click the Actions icon (three dots), and then click **Download**.
4. Review the **Terms of Use**.
5. Check the box labeled **I have reviewed and accept these terms and conditions**, then click **Download File**.

Determining the IP Address of Cloud EPM and Cloud EDM Environments

Environment URLs connect to static IP addresses. You may add these IP addresses to the allowlist in your firewall configuration to ensure that connections to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management can pass through the firewall.

Use a diagnostic tool such as ping or network administration tool such as nslookup to determine the IP address of each environment for which you want to add a pass through exception in the firewall configuration.

- **Sample ping command:** `ping serverName`, for example, `ping exampleServer.oraclecloud.com`
- **Sample nslookup command:** `nslookup serverName`, for example, `nslookup exampleServer.oraclecloud.com`

Be sure to specify only the fully-qualified server name available in the URL. All other information such as the protocol (https://) and application context (epmcloud) should be excluded. For example, if the URL is `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/epmcloud` use `acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com` as the server name.

Troubleshooting

See Resolving IP Allowlist Functional Issues in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Managing Navigation Flows

Service Administrators can set up cross-subscription connections called Navigation Flows that enable users to navigate across Oracle Fusion Cloud Enterprise Performance Management environments to create unified business process flows across multiple environments.

Navigation Flows allow users of multiple Cloud EPM environments to sign into one environment, and then seamlessly navigate to others without going through additional authentication processes. Service Administrators can create mash-ups of artifacts from various environments into a single unified business process flow for their users. Clusters, cards, and tabs can be brought together into a single flow. These cards and tabs can contain forms, reports dashboards from various applications.

Watch this video for an overview of customizing workflow in Cloud EPM.

 Overview Video

Considerations

- Navigation Flows can be created in the following business processes only:
  - Planning
  - Planning Modules
  - Financial Consolidation and Close
  - Tax Reporting
  - Enterprise Profitability and Cost Management
- All Cloud EPM environments can be accessed from these source connections. Navigation Flows can be created between environments of the same service type. Only connections where environments are in the same identity domain within the same region are supported.

> **Note**
>
> - Connections across environments that use different identity domains within the same region is not currently supported.
> - Applications must be of the same version. For example, you cannot set up connections between a 25.01 Planning application and a 24.12 Financial Consolidation and Close application.
> - You cannot use custom (vanity) URLs in Navigation Flows.

For detailed information on setting up and using Navigation Flows, see the Administration Guide of the source service in which you want to configure navigation flows. For troubleshooting information, see Handling Cloud EPM Connections Issues in *Operations Guide*.

Understanding Security Compliance Features

Oracle employs a multi-faceted approach to ensure Oracle Fusion Cloud Enterprise Performance Management security and to protect the confidentiality, integrity, and availability of data.

In addition to physical security of data centers, Oracle has implemented the following security compliance features. These features help you satisfy the security compliance requirements of your organization.

- Transport Layer Security (TLS) 1.2 and 1.3 for Communication
- Periodic TLS Certificate Renewal
- Data Encryption Using Transparent Data Encryption

- Data Encryption Using OCI Block Volume Encryption
- Encryption Keys Stored in FIPS 140-2 Compliant HSM
- Password Encryption for Secure EPM Automate Access
- Secure Storage of User Credentials
- Data Masking
- Data Isolation
- Externalized Authentication (Single Sign-On)
- Synchronize Users and Groups Using SCIM
- Use of APIs and Commands to Manage Access
- Use of OAuth 2 Tokens for REST APIs, EPM Automate, and EPM Integration Agent
- Multiple Password Policies
- API Gateway Support for REST APIs and EPM Automate
- Role-Based Access Control For End Users
- Virus Scan on Uploaded Files
- Block Upload of Files with Invalid File Extensions
- Network Restricted Access
- Immutable Backup Archive
- Air-Gapped Backup in a Secondary Region
- Setup IP AllowList for Connections
- Deactivate Access to Environments
- Sign-On Policies to Restrict Access to Environments
- Maximum Session Duration
- Idle Session Timeout
- Protection Using Web Application Firewall (WAF)
- Compliance with Oracle Global Trade Policy
- Secure HTTP Headers
- DKIM Support
- SPF Support
- DMARC Support
- Bring Your Own Key Functionality for Database Access
- Control Manual Database Access
- Monitor Manual Database Access
- Restrict Data Access by Oracle
- Access Log for Information on Each Access to the Environment
- Audit Reports, Login Reports, and Audit Logs
- User Login Report for Security Audit
- Activity Report to Monitor Application Performance
- Integration with Custom SIEM Tools

- Oracle Software Security Assurance (OSSA)
- Oracle's Monitoring of Environments Using Realtime Dashboards and Alerts
- Threat and Vulnerability Management
- Secure Access to Cloud Environments by Oracle
- Automatic Security Patching
- Periodic Penetration Testing and Ethical Hacking to Identify and Fix Vulnerabilities
- External Security Audits
- Customer-Initiated Security Testing
- Backup Data Residency and Retention
- 24X7 Support
- Security Policies for the United States Government
- Security Policies for the United Kingdom Government

Transport Layer Security (TLS) 1.2 and 1.3 for Communication

To satisfy the requirement of encrypted data communication, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management uses TLS 1.2 and 1.3 with strong ciphers to secure communication with browsers, Oracle Smart View for Office, EPM Automate and EPM Agent. All sessions are encrypted. Session information stored in cookies is encrypted and the session ID is randomly generated to ensure security.

Cloud EPM and Cloud EDM environments support the following ciphers:

- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- TLS_AES_256_GCM_SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-CCM
- ECDHE-ECDSA-AES128-CCM
- ECDHE-RSA-AES256-GCM-SHA384
- TLS_AES_128_CCM_SHA256

See these information sources for more information:

- Understanding Encryption Levels.
- Overview of Load Balancing in *Oracle Cloud Infrastructure Documentation*.

Periodic TLS Certificate Renewal

To satisfy the requirement of periodic certificate renewal, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management automatically renew TLS certificates every 6 months. The process is seamless and does not disrupt the operations of different interfaces, such as web browsers, Oracle Smart View for Office, EPM Automate, and EPM Agent.

If you are using an integration product that requires you to download certificates, do so every 6 months based on the certificate expiry date.

Data Encryption Using Transparent Data Encryption

To satisfy the requirement of encryption of data-at-rest, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management use Transparent Data Encryption (TDE) to encrypt all data at the tablespace level. Each tablespace has its own encryption key.

Encryption keys are encrypted using a master key. The master key is encrypted using AES-256 encryption and is rotated regularly. The master key is stored in a Hardware Security Module (HSM) for additional security.

Tablespace is also encrypted using AES-256 encryption.

Data Encryption Using OCI Block Volume Encryption

To satisfy the requirement of encryption of data at rest, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments use Block Volume Encryption using AES-256 to encrypt all file system data (including Oracle Essbase data).

Encryption Keys Stored in FIPS 140-2 Compliant HSM

To satisfy the requirement of encryption key storage in Hardware Security Module (HSM) in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments, all master keys including the following are stored in Federal Information Processing Standard (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

Password Encryption for Secure EPM Automate Access

You can mandate the use of an encrypted password file to satisfy the requirement of avoiding the use of plain text sensitive information while signing into EPM Automate. The data that can be encrypted include the system password (not the SSO password) and proxy server password. You use the encrypt EPM Automate command to create a file that stores the encrypted password.

Secure Storage of User Credentials

All user credentials are stored in a secure format using AES-256 encryption. This includes the following:

- Credentials provided while signing on
- Credentials supplied during the creation of navigation flows
- Credentials supplied during the creation of data source connections
- Credentials encrypted by EPM Automate encrypt command

Data Masking

These Oracle Fusion Cloud Enterprise Performance Management business processes support the masking of application data to ensure data privacy. This feature is especially useful when you need to hide application data before submitting snapshots to Oracle for troubleshooting.

- Planning application types including Custom, FreeForm , Planning Modules, Predictive Cash Forecasting, Strategic Workforce Planning, and Sales Planning.
- FreeForm
- Financial Consolidation and Close
- Enterprise Profitability and Cost Management
- Tax Reporting

You use the maskData EPM Automate command to hide sensitive data from application developers or from Oracle support when submitting snapshots. When executed, the command permanently replaces existing application data with randomized values, making it meaningless. This action cannot be reversed. If you create a snapshot after running the `maskData` command, the snapshot will contain only masked data.

If you need to submit a masked snapshot to Oracle but later restore the original data, you must do so from a backup or the daily maintenance snapshot created before masking.

Masking data helps you satisfy the requirement of not allowing your data to be visible to any other organization (in this case, Oracle).

Data Isolation

Oracle uses a dedicated virtual machine and a dedicated database schema for each customer to ensure that there is no mingling of data. This helps you satisfy data isolation requirements.

Externalized Authentication (Single Sign-On)

You can setup SSO to enable a SAML 2.0 compliant identity provider (IdP) to authenticate users for Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

This configuration satisfies the requirement of ensuring that users can no longer access Cloud EPM and Cloud EDM after leaving the organization. Since users login using the same SSO credentials that they use for network resources, removing their access to Cloud EPM and Cloud EDM is as simple as revoking their network access.

Additionally, communication between Oracle Access Manager, the default service provider for Cloud EPM and Cloud EDM, and your SAML 2.0 IdP is secured with the MD5 algorithm.

For detailed information on configuring SSO, see Configuring Single Sign-On.

Synchronize Users and Groups Using SCIM

To satisfy the requirement of centralized user and group management, you can use System for Cross-domain Identity Management (SCIM) to synchronize users and groups from other identity management solutions—such as another instance of Identity Cloud Service or Microsoft Entra ID—into your Oracle Identity Cloud Service instance that comes with Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data

Management. This synchronization is particularly valuable for unifying Cloud EPM and Cloud EDM environments that were initially set up with different identity domains.

For detailed information on synchronizing users and groups, see Using SCIM to Synchronize Users and Groups on Oracle Identity Cloud

Use of APIs and Commands to Manage Access

If SSO is not configured for Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management, you can satisfy the requirement to ensure that only authorized users can access these environments by using REST APIs and EPM Automate commands. These tools allow you to add users, assign them to predefined and application roles, and add them to groups. Use of EPM Automate commands and REST APIs to administer users, groups, and role assignments are simple but secure operations that help ensure that only authorized users have access to the environments.

For information on using EPM Automate commands and REST APIs, see these information sources:

- *Working with EPM Automate*
- *REST APIs for Oracle Fusion Cloud EPM*

Use of OAuth 2 Tokens for REST APIs, EPM Automate, and EPM Integration Agent

You can use OAuth 2 access tokens to make REST API calls to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management and to use EPM Automate and the EPM Integration Agent to satisfy the requirement of avoiding the use of passwords in your environments. See:

- Using OAuth 2.0 Authorization Protocol with OCI in *Working with EPM Automate*.
- Authentication with OAuth 2 - Only for OCI in *REST APIs for Oracle Fusion Cloud EPM*.

Multiple Password Policies

To satisfy the requirement of multiple password restrictions for different users, groups, and roles, you can create multiple password policies and assign them to different IDCS groups. A user belonging to an IDCS group will use the password policy assigned to that group. For details, see Manage Oracle Identity Cloud Service Password Policies in *Administering Oracle Identity Cloud Service*.

API Gateway Support for REST APIs and EPM Automate

To satisfy the requirement of API Gateway support, Oracle Fusion Cloud Enterprise Performance Management REST APIs and EPM Automate can connect to Cloud EPM and Oracle Fusion Cloud Enterprise Data Management through API Gateways, such as Google APIGEE, IBM Data Power, and other reverse proxy servers.

Role-Based Access Control For End Users

Access to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management is strictly controlled through the use of predefined roles. These

roles determine the functional access each user. For detailed information on predefined roles, see Understanding Predefined Roles.

Additionally, Service Administrators can use Access Control to create groups comprising identity domain users or other groups. Assigning roles to such groups enables Service Administrators to grant roles to many users at once, thereby reducing administrative overheads. Assigning roles at the application-level can only enhance the access rights of users; none of the privileges granted by a predefined role can be curtailed by roles assigned at the application-level. This satisfies your role-based access control (RBAC) requirements.

For more information on Access Control, see "Overview of Access Control" in *Administering Access Control*

Virus Scan on Uploaded Files

To satisfy the requirement of uploaded files to be scanned for virus, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management 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.

Refer to the following guides to enable virus scanning using REST APIs or EPM Automate commands:

- *REST APIs for Oracle Fusion Cloud EPM*
  - Get Virus Scan on File Uploads
  - Set Virus Scan on File Uploads
- *Working with EPM Automate*:
  - Get Virus Scan On File Uploads
  - Set Virus Scan On File Uploads

Block Upload of Files with Invalid File Extensions

To satisfy the requirement of blocking the invalid file extensions of uploaded files, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments do not allow uploading of the files with invalid extension. This is enforced in all user interfaces that allow uploading files, including browser interface, EPM Automate, and REST APIs.

Network Restricted Access

To satisfy the requirement of not allowing unauthorized access to your data, you can configure an allowlist or a blocklist to control access to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments based on source IP addresses.

- An **allowlist** specifies which IP addresses are permitted to access an environment.
- A **blocklist** defines IP addresses that are explicitly denied access.

These controls help ensure that only trusted networks can interact with your environments.You can configure the allowlist for the entire IAM domain. See Setting up Network Perimeter.

Immutable Backup Archive

To ensure that daily snapshots cannot be modified after they are archived, Oracle makes the archived daily backups in Oracle Object Storage immutable. This means the backups can be retrieved but not altered or updated.

Air-Gapped Backup in a Secondary Region

To ensure advanced data protection, Oracle creates air-gapped backups of snapshots in Oracle storage buckets in secondary regions. Such backups ensure the survivability of data in case of a production site outage and minimize unauthorized access opportunities. For information on the backup site for each region, see OCI (Gen 2) Geographical Regions and Identifiers in *Oracle Enterprise Performance Management Cloud Operations Guide.*

Setup IP AllowList for Connections

You can satisfy the requirement of allowing access to your cloud environments from only specific IP addresses. Add the outbound IP addresses of the regions where your Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments are hosted to the Network Perimeter. For reference, see Outbound IP Addresses of EPM Cloud Data Centers and Regions in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Enable Cloud EPM and Cloud EDM to Accept Connections from Other Cloud EPM and Cloud EDM Environments

Once the Network Perimeter is configured, your environment will, by default, block incoming connections from other Cloud EPM and Cloud EDM environments.

To permit access from a specific environment, add the outbound IP addresses of the region hosting the requesting environment to the Network Perimeter.

For example, if you are executing `copySnapshotFromInstance` EPM Automate command from an environment that has Network Perimeter configured, the outbound IP addresses of the region where the source environment is located must be added to the Network Perimeter.

This also applies to:

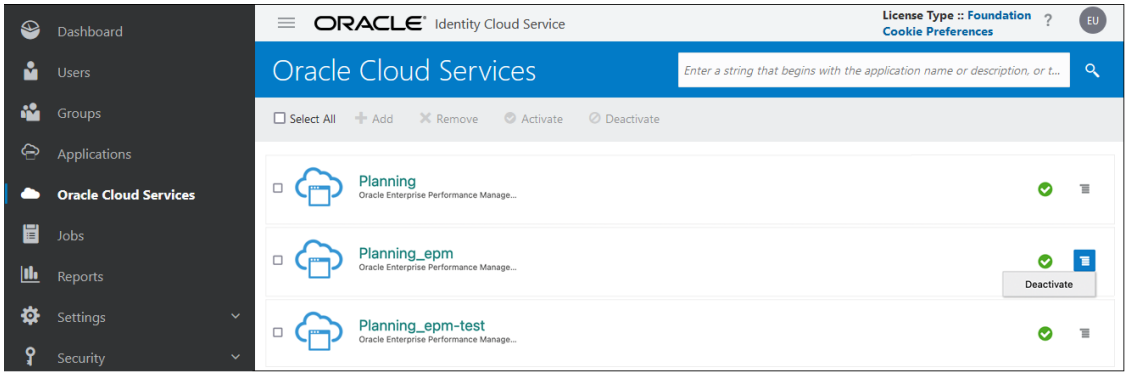
- Copy Application Snapshot REST API
- Cloning Cloud EPM Environments screen in Migration tool
- `cloneEnvironment` EPM Automate command
- Clone an Environment REST API
- Navigation Flows

Enable Fusion or NetSuite to Accept Connections from Cloud EPM and Cloud EDM

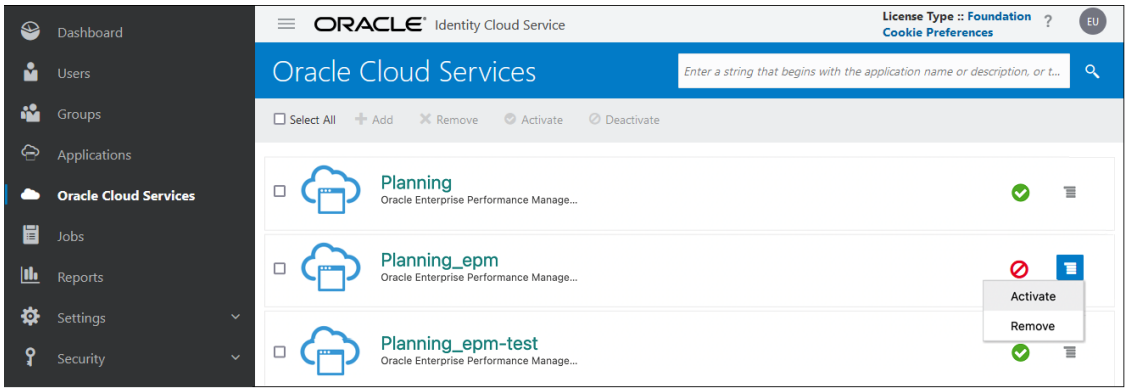
After configuring the AllowList on a Fusion or NetSuite environment, access from Cloud EPM and Cloud EDM will be blocked by default. To grant this access, update the IP AllowList in the Fusion or NetSuite environment to include the outbound IP addresses of the region where Cloud EPM and Cloud EDM environments are located.

Deactivate Access to Environments

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments can be deactivated so that no user can log in to them. This feature can be used 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.



You can reactivate a deactivated environment whenever you so choose.



Sign-On Policies to Restrict Access to Environments

The default sign-on policy in Oracle Identity Cloud Service allows all users assigned to predefined roles to sign into environments by supplying their credentials (user name and password). Identity Domain Administrators may configure a custom sign-on policy to determine whether a user is allowed to access Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. For example, you may configure a policy that allows only users assigned to the Service Administrator role to access environments.

For detailed information on configuring sign-on policy, see these topics in *Administering Oracle Identity Cloud Service*:

- Understand Sign-On Policies
- Add a Sign-On Policy

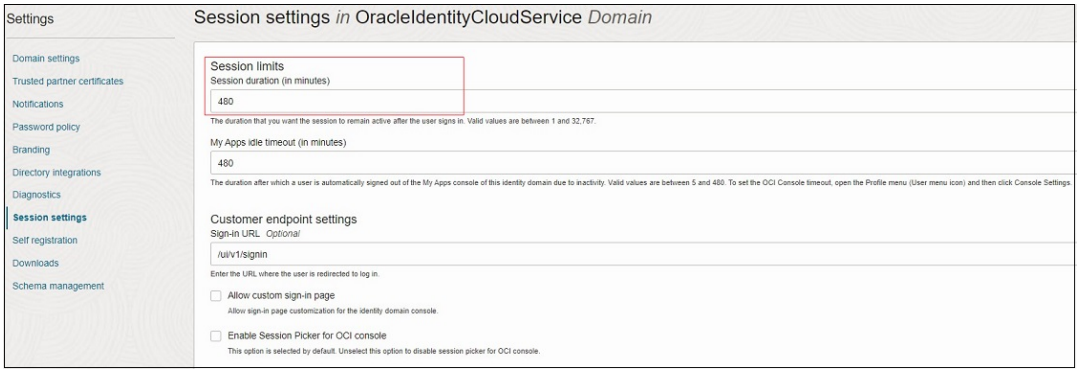
Maximum Session Duration

To satisfy the requirement of limited session duration, the Identity Domain Administrator can set the maximum session duration. Follow the instructions below to set the maximum session duration:

> **Note**
>
> The maximum session duration is not the same as the idle session timeout. Even if the session is active, the users will be logged out after the maximum session duration is reached.

1. Go to IAM Interface. See Accessing the IAM Interface
2. Click **Settings** in the left navigation panel.
3. To set session timeout, in **Session duration (in minutes)**, enter the desired duration that a user session can remain active. After this duration, the user's session, even if active, will be timed out.
4. To set idle session timeout of My Apps console, in **My Apps idle timeout (in minutes)**, enter the desired duration that an idle user session in My Apps console can remain active.

> **Note**
>
> **My Apps idle timeout (in minutes)** does not change the Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment's idle session timeout. For instructions on changing the environment's idle session timeout, see Changing Idle Session Timeout Settings.



Idle Session Timeout

To satisfy the requirement of sessions timeout due to inactivity, Service Administrators can set the idle session timeout settings in the environments. For instructions, see Changing Idle Session Timeout Settings.

Protection Using Web Application Firewall (WAF)

The Web Application Firewall (WAF) satisfies the requirement to provide out-of-box protection for Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management from a variety of application layer attacks, such as cross-site scripting and SQL injection.

Compliance with Oracle Global Trade Policy

In compliance with the Oracle's worldwide trade compliant business policies, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management enforce Oracle Global Trade Policy (GTC), including restricting access from the Embargo countries.

Secure HTTP Headers

To satisfy the requirement of secure HTTP headers, all HTTP requests and responses in Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environments include the following secure HTTP headers:

HTTP Request Headers

- WL-Proxy-Client-IP
- WL-Proxy-SSL
- IS_SSL

HTTP Response Headers

- Strict-Transport-Security
- X-Content-Type-Options
- Secure
- samesite
- Referrer-Policy
- Permissions-Policy
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies

DKIM Support

To satisfy the requirement of DKIM (DomainKeys Identified Mail) support, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments support DKIM functionality. Cloud EPM and Cloud EDM email servers sign outgoing messages using a private key, while receiving mail servers verify these signatures with a public key published in the `oraclecloud.com` DNS record.

Additionally, Cloud EPM and Cloud EDM environments also support DKIM with custom sender email address. For instructions on requesting outgoing messages to use DKIM-compliant custom sender email address, see Request Custom Sender Email Address for OCI (Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide* .

.

SPF Support

To satisfy the requirement of SPF (Sender Protection Framework) support, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management 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. Refer to Configuring SPF Record for Email Verification for details.

DMARC Support

To satisfy the requirement of DMARC (Domain-based Message Authentication, Reporting, and Conformance) support, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments create DMARC-compliant emails. These emails pass SPF authentication and SPF alignment as well as DKIM authentication and DKIM alignment.

Bring Your Own Key Functionality for Database Access

You use the setEncryptionKey EPM Automate command to specify a custom encryption key for accessing the data in the database. Using this command provides you a bring your own key solution that will include Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management in your standard key management and satisfies the requirement of using your own key management.

Control Manual Database Access

By default, Oracle is permitted to manually access the databases of Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments during emergency situations when the environment is unresponsive and customer has not yet submitted a service request for investigation and restoration.

You can prevent such manual database access by revoking manual data access using the setManualDataAccess EPM Automate command. If this access is revoked, Oracle cannot execute SQL commands against the tablespace under any circumstance without your explicit permission (allowing manual access) using the `setManualDataAccess` command. This helps you satisfy the requirement of not allowing unauthorized access to your data.

Monitor Manual Database Access

You can satisfy the requirement of monitoring access to your database by analyzing the Manual SQL Execution table in the Activity Report. This report identifies the SQL statements that were executed against the database and indicates why each statement was run.

Restrict Data Access by Oracle

To satisfy the requirement of restricted data access, you can prevent Service Administrator from submitting application snapshot to Oracle. To do so, set the restricted data access to true using the following EPM Automate command or REST API:

- Set Restricted Data Access in *REST API for Enterprise Performance Management Cloud*

- setRestrictedDataAccess in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*

> **Note**
>
> Service Administrators cannot submit application snapshots to Oracle in restricted OCI regions (for example, regions in OC2 and OC4 realms).

Access Log for Information on Each Access to the Environment

To satisfy the requirement of monitoring every access to your Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments, an Access Log is automatically created and maintained . This log includes information about users who logs into the environment directly or by using tools such as EPM Automate. Monitoring the Access Logs helps Service Administrators understand application usage by each active user. See these topics:

- Activity Report Contents
- Viewing and Downloading Activity Reports and Access Logs

Audit Reports, Login Reports, and Audit Logs

Multiple reports are available in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments to audit user, role, and group modifications.

- Role Assignment Audit Report - Audits the changes made to predefined and application role assignments. Available via:
  - The roleAssignmentAuditReport EPM Automate command.
  - The Role Assignment Audit Report for OCI REST API.
- Group Assignment Audit Report - Audits the addition and removal of users and groups to or from Access Control groups. Available via:
  - The groupAssignmentAuditReport EPM Automate command.
  - The Group Assignment Audit Report REST API.
- User Audit Report - Audits the users who signed into the environment successfully. Available via:
  - The userAuditReport EPM Automate command.
  - The User Audit Report REST API.
  - The User Login Report in EPM Automate.
- Invalid Login Report - Audits the failed attempts to sign into the environment. Available via:
  - The invalidLoginReport EPM Automate command.
  - The Invalid Login Report for OCI REST API.

In addition, Identity Cloud Service provides you audit and login reports such as the following:

- Audit log containing information on successful and failed logins, and user management actions: user creation, update, and deletion

- Application Role Privileges Report, which can be used as an audit report for all predefined role modifications
- Successful Login Attempts Report
- Unsuccessful Login Attempts Report
- Dormant Users Report

For information on these reports, see Audit and Login Reporting Overview.

User Login Report for Security Audit

To satisfy the requirement of monitoring user access to the environment, you can review the User Login report, which tracks the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management usage by each authorized user. This report contains information on users who signed in over the last 24 hours, including the IP address of the computer from used for login in and the date and time (UTC) of access.

You can regenerate this report for a custom date range or for the last 30 days, last 90 days, and last 120 days. You can also filter the report to view only the information of specific users by using a partial string of the users' first name, last name or userID as the search string.

For detailed steps to create the User Login report, see "Viewing the User Login Report" in *Administering Access Control*.

Activity Report to Monitor Application Performance

To satisfy the requirement of application monitoring, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management automatically creates and store a daily Activity Report, that displays the environment's performance from the application point of view. For detailed information, see these topics:

- Activity Report Contents
- Viewing and Downloading Activity Reports and Access Logs

Integration with Custom SIEM Tools

To satisfy the requirement of integration with SIEM (Security Information and Event Management) tool of your choice, you can download the Access Log every day and forward it to SIEM tool.

The Access Log contains information on all users who logged into the environment directly, or by using tools such as EPM Automate. It includes information on IP address, username, date and time, and the functionality that was executed by the user. Forwarding it to SIEM tool provides you the capability to include access to your Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments in the SIEM analysis and filtering capabilities. See Download Access Logs from an Environment in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*.

Oracle Software Security Assurance (OSSA)

From a security evaluation perspective, Oracle is committed to international standards such as FIPS, a cryptographic module validation scheme, and ISO standards. Oracle's Global Product Security promotes and monitors the adoption of Oracle Software Security Assurance (OSSA) policies and practices. These include Oracle Secure Coding Standards (SCS), Critical Patch

Update (CPU) and Security Alert programs. These programs satisfy your security compliance requirements related to secure coding, security patches, and so on.

Oracle's Monitoring of Environments Using Realtime Dashboards and Alerts

To satisfy the requirement of continuous monitoring, Oracle monitors all Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments in real-time and send appropriate alerts to Oracle Operations and Development teams. Oracle utilizes various dashboards to monitor the health of the environments and to provide visual alerts. Oracle Operations and Development teams work around the clock to rectify the alerts, ensuring that your environments are operating as designed and are secure.

Threat and Vulnerability Management

To satisfy the requirement of threat and vulnerability management, Oracle uses QualysGuard from Qualys to discover and scan the IT infrastructure and Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management applications for security vulnerabilities and malware. QualysGuard delivers security intelligence data that aids with Oracle's security compliance processes.

Use of QualysGuard ensure that internet-facing servers, websites, and web applications are up to date and securely configured against malicious attacks. It also helps ensure that no uploaded malware exists in blogs and forum pages, and that web forms do not include potential hacking risks.

To prevent risks to our customers, Oracle does not provide additional information about the specifics of vulnerabilities beyond what is provided in the penetration test summaries. Oracle provides its customers with the same information to protect all customers equally. Oracle does not provide advance notification to individual customers. Finally, Oracle does not develop or distribute active exploit code (or proof of concept code) for vulnerabilities in our products. See Oracle Security Vulnerability Disclosure Policies.

Secure Access to Cloud Environments by Oracle

Oracle requires to access your environments to troubleshoot issues. This access is highly secure and tightly regulated. Only a select group of Oracle employees, trained specifically in handling customer environments, are permitted access to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management. All access is protected by multi-factor authentication and is subject to auditing.

Automatic Security Patching

Oracle issues security alerts and fixes all identified critical security concerns as soon as they are identified. Non-critical Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management issues are fixed through the monthly update to the environment. Automatic security patching helps you satisfy the requirement of applying current security patches.

Periodic Penetration Testing and Ethical Hacking to Identify and Fix Vulnerabilities

Oracle employs third party security teams to perform periodic penetration testing. Oracle also employs a dedicated team of ethical hackers who engage in the in-depth hacking of the Oracle code base. These tests ensure that there are no vulnerabilities. Any vulnerability found is

immediately reported to the Development team and rectified. Oracle makes the security testing reports available to you. Penetration testing and ethical hacking are designed to satisfy your requirement of security penetration testing and reports.

External Security Audits

Oracle engages third parties to independently conduct security audits of Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management and create security reports, for example, SOC 1 reports (based on Statement on Standards for Attestation Engagements (SSAE) No 18), SOC 2 reports, and other independent third party reports to review the effectiveness of administrative and technical controls. The following reports are available to you in the Oracle Cloud Console (See Accessing Compliance Reports) to satisfy your compliance requirements:

- SOC 1 Report
- SOC 2 Report
- Bridge Letter
- ISO Certificate
- Disaster Recovery Evidence Document
- Security Assessment Report

Customer-Initiated Security Testing

Oracle conducts security testing and engages third parties for additional assessments. However, customers who wish to perform their own security testing or engage a third party to conduct testing on their Oracle Fusion Cloud EPM environments must obtain prior approval from Oracle. Approval is granted based on regulatory requirements to comply with specific applicable regulations.

For instructions on how to request approval, refer to Security Testing in the Oracle Cloud.

Backup Data Residency and Retention

Every day, during the operational maintenance of the environment, Oracle backs up the content of the environment to create a maintenance snapshot, named Artifact Snapshot, of existing artifacts and data. The maintenance snapshot can be used to recover artifacts and data and to restore the environment to the state it was in during the last operational maintenance. For detailed information on the maintenance snapshot and retention policy, see Overview of the Maintenance Snapshot.

Daily snapshots are archived to Oracle Object Storage. Production and test environment snapshots are retained for 60 days. This satisfies your backup and archive requirements.

The daily snapshots from the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments are archived to Oracle Object Storage within the same OCI region as the environment. This satisfies the requirement that the data on the Cloud EPM and Cloud EDM environments does not leave the region.

> **Note**
>
> Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. For the availability domains of different OCI regions, refer to Regions and Availability Domains.

Oracle Object Storage is designed to be highly durable, providing 99.999999999% (Eleven 9s) of annual durability. It achieves this by storing each object redundantly across three different availability domains for regions with multiple availability domains, and across three different fault domains in regions with a single availability domain. Data integrity is actively monitored using checksums, and corrupt data is detected and automatically repaired. Any loss in data redundancy is detected and remedied, without customer intervention or impact.

If you have a requirement to archive backups to another region and/or for longer duration, you can use self-service automation scripts to replicate the backups to other OCI regions and/or archive them for longer duration.

Sample scripts for backing up snapshots are available in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud* :

- See Back up Application Snapshot to a Computer for a sample script for downloading daily snapshots and storing them in an on-premise storage.
- See Copying a Snapshot to or from Oracle Object Storage for a sample script for archiving daily snapshots in Oracle Object Storage.

24X7 Support

To satisfy the requirement of continuous monitoring, Oracle Cloud Operations specialists monitor and support all key aspects of Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management including applications, middleware, database, and infrastructure. All cloud operations are performed by Oracle badged employees without any involvement by third parties.

Alerts are monitored 24x7 across the globe. The Oracle Operations team is dedicated to handling maintenance activities and unplanned outages and incidents and providing accurate, and timely information to internal and external stakeholders around outages and incidents. Oracle employs a tiered structure for issue resolution. Based on the complexity of the issue, experts from all over the world are within a moment's reach for timely resolution.

Within Oracle Fusion Cloud EPM Operations, a dedicated team of hundreds of specialists handle security operations. The activities of this team include building internal tools to maintain and enhance the existing architecture, ensuring compliance with the most recent frameworks such as GDPR, policy enforcement (for example, disaster recovery testing), and design and development of the security practices (for example, system hardening procedures).

Security Policies for the United States Government

To satisfy the stringent requirements of US public sector, Oracle has established isolated FedRAMP ready Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments strictly for United States public sector customers such as local, state and federal agencies, colleges and universities, national laboratories, and government contractors. These environments provide advanced data security

controls that aligns with NIST 800-37(Guide for Applying the Risk Management Framework to Federal Information Systems) and FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) as mandated by the Federal Information Security Management Act. These standards ensure greater data privacy and protection.

For public sector customers, data is processed and stored in the US. All activities are handled by US Citizens.

Security Policies for the United Kingdom Government

To satisfy the stringent requirements of UK public sector, Oracle has established isolated and highly secure Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments strictly for United Kingdom public sector customers such as local, state and federal agencies, colleges and universities, national laboratories, and government contractors. For these customers, data is processed and stored in the UK. Access it restricted to UK citizens residing in the UK.

Environments dedicated for the use of UK public sector have Cyber Essentials Plus Certification; they align with ISO 27001 and Cloud Security Principles. Oracle provides support by a UK Cloud Operations public sector compliance analyst to assist with initial assessment against the Supplier Assurance Framework and Cloud Security Principles.

9

Backing Up and Restoring an Environment Using the Maintenance Snapshot

Oracle uses `Artifact Snapshot` to restore artifacts and data. This snapshot is created by the daily maintenance process.

In This Section:

Overview of the Maintenance Snapshot

Every day, during the operational maintenance of the environment, Oracle backs up the content of the environment to create a maintenance snapshot, named `Artifact Snapshot`, of existing artifacts and data.

Service Administrators can use the maintenance snapshot to recover artifacts and data; for example, form definitions, reports, and so on, from the previous day that were deleted from the service after the last operational maintenance window. They can also, if needed, use it to restore the environment to the state it was in during the last operational maintenance. See Setting the Maintenance Start Time for an Environment.

Note

- An environment does not create a maintenance snapshot if it has not been in use since the last maintenance window. If an environment has not been in use for 14 days, however, a new maintenance snapshot is created.
- Generally, you can migrate maintenance snapshots from the test environment to the production environment and vice versa.
  Account Reconciliation and Enterprise Data Management (business process and cloud) do not support migration of snapshots from the latest service update to an earlier service update (for example, when moving snapshots between test and production environments during the window when the test environment is upgraded before the production environment).
- You can create a backup of your environment at any time by exporting artifacts using Migration. See "Backing up Artifacts and Applications" in *Administering Migration*.
- The business process is placed in the maintenance mode when the daily maintenance of the environment starts. See Managing Daily Maintenance.

These Artifacts are Not Included in the Maintenance Snapshot

- Files that were uploaded to the environment, including snapshots that you uploaded.
- Files that you created by exporting artifacts from the environment.
- Audit data. Snapshots of all business processes other than Planning, Planning Modules, Profitability and Cost Management, and Enterprise Profitability and Cost Management include audit information.
- Job Console data. For Planning, Planning Modules, FreeForm, and Enterprise Profitability and Cost Management, job console data is not included in the snapshot.
- Data Management Staging Table Data. Using the LCM Mode feature, customers can take a snapshot of staging table data from the Workbench. To export and import this data, use the exportDataManagement and importDataManagement EPM Automate commands or the Data Management System Maintenances Scripts interface.

To create an identical copy of an environment, including audit data, job console data, Data Management staging table data, and stored snapshots and files, use the cloneEnvironment EPM Automate command or the Clone Environment feature.

About the XML Files in the Snapshot

The XML files included in the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management snapshots use an Oracle defined proprietary format. This format may change to accommodate changes that occur over the releases. Any custom process or utility that you use should not depend on the XML format remaining unchanged across all releases.

Managing Maintenance Snapshots

Maintenance snapshots are created primarily to restore your environment in the case of a catastrophic failure.

All files and snapshots that you create or upload to Cloud EPM and Cloud EDM environments are deleted after 60 days. A daily maintenance process monitors the environments and automatically removes snapshots older than 60 days. If the total size of the remaining snapshots exceeds 150 GB, it deletes snapshots created in the last 60 days but older than 48 hours, starting with the oldest, until the total size is below 150 GB. The daily maintenance snapshot is always retained, regardless of its size. If this maintenance snapshot exceeds 150 GB, only it will be retained; and all other snapshots will be deleted.

The daily snapshot is then archived with the retention policy described in Archival, Retention, and Retrieval of Daily Snapshots.

Exceptions

- Narrative Reporting retains only the current snapshot (`EPRCS_Backup.tar.gz`) of the environment.
  Thus, the 150 GB limit is not applicable to Narrative Reporting, but retention period for files and uploaded artifacts is enforced.
- Data Management process log files are retained for seven days only.

Archival, Retention, and Retrieval of Daily Snapshots

Daily snapshots are archived every day to Oracle Object Storage. Production and test environment snapshots are retained for 60 days. You can use 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 for the last 60 days for both production and test environments.
It is your responsibility to archive backups for any duration your organization requires. To do so, you download daily snapshots using the downloadfile EPM Automate command and archive them to an on-premise or cloud storage. You can also archive snapshots in Oracle Object Storage using the copyToObjectStorage EPM Automate command.

Sample scripts for backing up snapshots are available in *Working with EPM Automate*. See:

- Back up Application Snapshot to a Computer for a sample script for downloading daily snapshots and storing them in an on-premise storage
- Copying a Snapshot to or from Oracle Object Storage for a sample script for archiving daily snapshots in Oracle Object Storage

Data Size in an Environment

In this Section:

What Contributes to the Data Size in an Environment?

Data size in a service environment is the sum of the following:

- Application data stored in Essbase.
- Artifact snapshot created by the daily maintenance process
- Snapshots that you created using Migration and EPM Automate.
- Snapshots that you uploaded using Migration and EPM Automate.
- Data and metadata files that you uploaded using Migration and EPM Automate.
- Attachments stored in the database (applicable to Account Reconciliation when not configured to use Object Storage for attachments)

> **Note**
>
> Daily maintenance snapshots archived in Oracle Object Storage do not contribute to the total reported application size. These have no size limits.

The Activity Report lists application size information including data size (includes the size of snapshots, and files available in the inbox and outbox), size of Essbase data, and the size of the maintenance snapshot. See Application Design and Runtime Information.

What is the Maximum Allowed Data Size in an Environment?

EPM Standard and EPM Enterprise Subscriptions: No maximum data size limit is imposed for EPM Standard and EPM Enterprise environments.

Other Subscriptions: The maximum allowed data size for an environment is 150 GB. Contact your Oracle Sales Representative if you want to increase this limit. Additional fees may apply.

> **Note**
>
> The data size does not include the size of the daily maintenance snapshots archived in Oracle Object Storage.

How Do I Determine the Current Size of Data in an Environment?

Use the Activity Report to determine the data size. See Application Size.

For Services Other than Narrative Reporting

You can download the daily maintenance snapshot to a local computer manually from the Migration screen or automatically by using EPM Automate.

- Backing up the Maintenance Snapshot
- Importing Snapshot to Restore Environment

Troubleshooting

See Resolving Import and Export, and Backup Errors in *Oracle Enterprise Performance Management Cloud Operations Guide.*

Backing up the Maintenance Snapshot

Automating the Download of the Maintenance Snapshot

To automate the downloading of the snapshot, you create a script file containing the required EPM Automate commands, and schedule it (for example, using Windows Scheduler or Linux cron job) to run after the daily maintenance of the environment is complete. See "Scenario 8: Backing up Application Snapshot to a Computer" in *Working with EPM Automate* for a sample Windows script that you can repurpose to download the artifact snapshot.

Copying a Snapshot to Oracle Object Storage

You can use the copyToObjectStorage EPM Automate command to copy a snapshot from an Oracle Fusion Cloud Enterprise Performance Management environment to an Oracle Object Storage Cloud bucket.

See these information sources in *Working with EPM Automate*:

- copyToObjectStorage
- copyFromObjectStorage
- Copying a Snapshot to or from Oracle Object Storage

Manually Downloading the Maintenance Snapshot

To manually download the artifact snapshot:

1. Access the environment as a Service Administrator. See Accessing Cloud EPM and Cloud EDM Environments.

You can sign in as a Service Administrator, or as a user with Migrations - Administer application role.

2. Complete a step:
   - Click **Tools** and then **Migration**.
   - **Profitability and Cost Management only:** Click **Application** and then  (Migration).
3. Click **Snapshots**.
4. Click ••• (Actions) next to **Artifact Snapshot**, and then select **Download**.
5. Save the artifact snapshot (`Artifact Snapshot.zip`) to the local computer.

Importing Snapshot to Restore Environment

You can restore application artifacts and data from previous snapshots. For example, you can restore the artifacts and data to the state they were in a few days ago by importing a snapshot that you backed up to a local machine.

Before importing, you should upload the source snapshot to the Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment. Snapshots that you create or upload to the service are stored for 60 days, after which they are automatically deleted. See these sources for information on uploading snapshots to an environment:

- The uploadFile EPM Automate command
- "Uploading Archives to the Service" in *Administering Migration*

Key Considerations

- Enterprise Data Management and Narrative Reporting do not support the migration of snapshots from a monthly update to a previous monthly update (for example, when moving snapshots between test and production environments during the window when the test environment is upgraded before the production environment). It supports migration only across the same monthly update or to the next monthly update.
- Account Reconciliation supports the migration of individual artifacts to a previous monthly update, except for the Application Snapshot artifact.
- All other business processes support the migration of snapshots from a monthly update to the previous and next monthly updates.
- Import operation may fail if Planning contains a renamed seeded period member that has been supplanted by a custom period member. For example, you renamed the seeded YearTotal Period member to unused_YearTotal and then added an alternate type period member with the original seeded member name (YearTotal in this example). In this scenario, import of snapshot into the business process may fail.

> **Note**
>
> You cannot import Oracle Essbase data by itself. Essbase data can only be imported as part of full snapshot import.

To restore artifacts from a snapshot:

1. Access the environment as a Service Administrator, or as a user with Migrations - Administer application role. See Accessing Cloud EPM and Cloud EDM Environments.

2. Complete a step:
   - Click **Tools** and then **Migration**.
   - **Profitability and Cost Management only:** Click **Application** and then  (Migration).
3. Click **Snapshots**.
4. Select the snapshot that you want to use as the source to restore artifacts.
   - **To restore all artifacts of a specific component:**
     a. Expand the snapshot, and then click a component name; for example `HP-Vision` to list artifacts of the Vision sample application included in the snapshot.
     b. Click **Import**.
   - **To restore specific artifacts of service components:**
     a. Expand the snapshot, and then click a component name; for example `HP-Vision` to access a list of artifacts of the Vision sample application included in the snapshot.
     b. In **Artifact List**, expand the list of available artifacts, and then select the artifacts you want to restore.
     c. Click **Close** to return to **Artifact Snapshots**.
     d. **Optional:** Repeat the preceding steps to select artifacts from other components included in the snapshot.
5. Click  (Selected Artifacts), and then verify the list of artifacts selected for export.
6. Click **Actions**, and then select **Import**.
7. Click **OK**.

   The Migration Status Report opens. Click **Refresh** to verify that the operation completes without errors. Click **Cancel** to close the report.

For Narrative Reporting Only

Narrative Reporting uses the `uploadFile` and `downloadFile` EPM Automate commands to perform backup and restore activities.

Downloading a Snapshot

Use the following EPM Automate command to download the database snapshot to a local computer:

```
EPMAutomate downloadFile EPRCS_Backup.tar.gz
```

For detailed information on this command, see downloadFile in *Working with EPM Automate*.

Uploading a Backup Snapshot to the Environment

Use the following command to upload a backup database snapshot from a local computer to a Narrative Reporting environment:

`EPMAutomate uploadFile EPRCS_Backup.tar.gz [to_be_imported]`, where `[to_be_imported]`, optionally, is a location in the Narrative Reporting environment. If it is not specified, the uploaded snapshot replaces the current daily maintenance snapshot. If this location is specified, `EPRCS_Backup.tar.gz` will be imported during the next maintenance of the environment.

For detailed information on this command, see uploadFile in *Working with EPM Automate*.

> **Note**
>
> Make sure that the destination environment is of the same release or newer. You cannot restore a backup snapshot into a service that has an older release. You can confirm the current version of the environment from the **Settings and Action** menu in the Home page.

Restoring an Environment from a Backup Snapshot

When you restore a backup snapshot, your environment returns to the state at which the snapshot was taken. Changes that occurred after the backup are not reflected in the restored environment.

Service Administrators can restore an environment from the current maintenance snapshot screen or from a backup uploaded from a local computer if the backup snapshot is of the same release as the environment or newer.

A backup snapshot that a Service Administrator uploads to the `to_be_imported` location in the Narrative Reporting environment is automatically restored during the next daily maintenance. You may schedule the next maintenance so that it starts soon after you upload the backup snapshot to `to_be_imported`. If daily maintenance includes restoring an application from a backup, the maintenance process may take more than one hour. The additional time requirement varies with the size of the snapshot being restored. See Setting the Maintenance Start Time for an Environment.

From the Daily Maintenance screen, a Service Administrator can restore an environment using the current maintenance snapshot.

To restore an environment from the current maintenance snapshot:

1. Sign into the environment.
2. On the **Home** page, click **Tools** and then **Daily Maintenance**.
3. Under **Restore Backup Snapshot**, select **Using the most recent daily backup**.
4. Click **Schedule Restore**.
5. Click **Yes** to restore the environment from the maintenance snapshot during the next daily maintenance.

10

Setting Up Cloud EPM and Cloud EDM Environments

In This Section:

Configuring Appearance

On the **Appearance** page, you can configure and customize your environments for easy recognition; for example, to distinguish your test environment from the production environments or to distinguish one service type from another.

Customizing Your Display

> **Note**
>
> Not all Oracle Fusion Cloud Enterprise Performance Management business processes offer identical customization options.

1. Access the environment as a Service Administrator. See Accessing Cloud EPM and Cloud EDM Environments.
2. Click **Tools** and then **Appearance**.
3. In the **Theme** drop-down menu, select the Oracle, Custom Dark, or Custom Light theme. See Themes.
4. In **Logo Image**, choose **Oracle**, select **Upload File,** or **Provide URL**. See Logo and Background Image Requirements.

5. In Custom Light or Custom Dark theme only:
   - In **Home Background Image**, choose **Default Texture**, select **Upload File**, or **Provide URL**. See Logo and Background Image Requirements.
   - In **Brand Color**, click the colored circle and select from one of the predefined colors for the pattern stripe image in the page header.
6. In **Display Business Process Name**, select **Yes** to display the business process name next to the logo on the Home page and on the tab when a browser tab is opened.
7. Click **Save**.

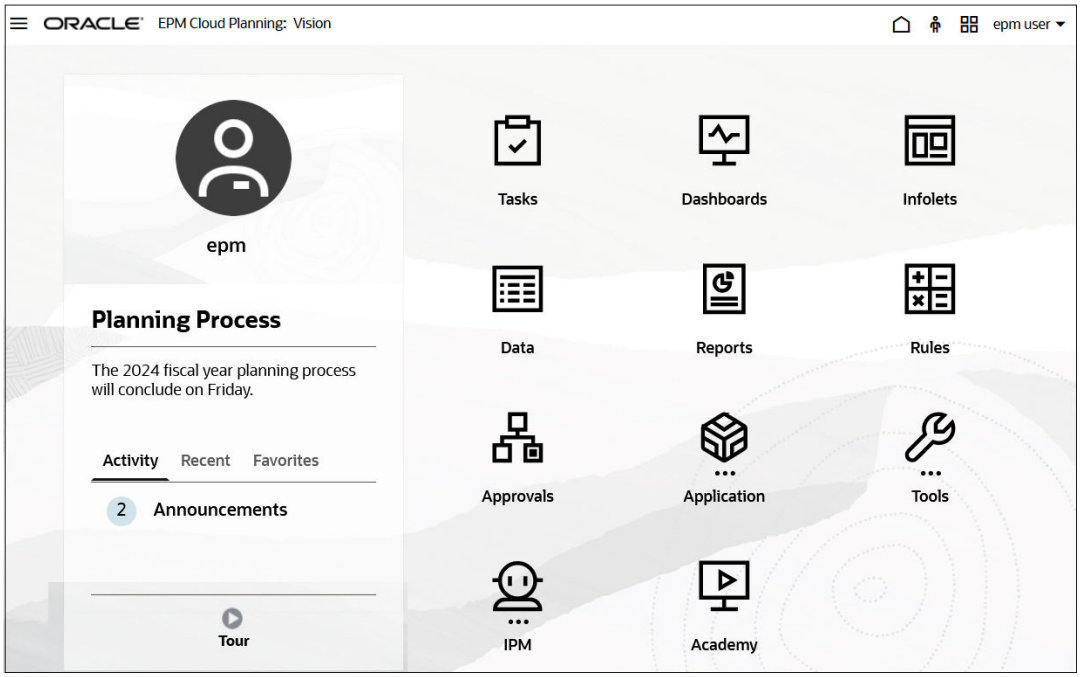
Themes

For optimal performance, Oracle recommends setting your Windows display scale to 125% or lower. To ensure smooth operation, Cloud EPM and Oracle Fusion Cloud Enterprise Data Management require access to `static.oracle.com` for image files, JavaScript, and other static content. Please ensure your firewall permits this access.

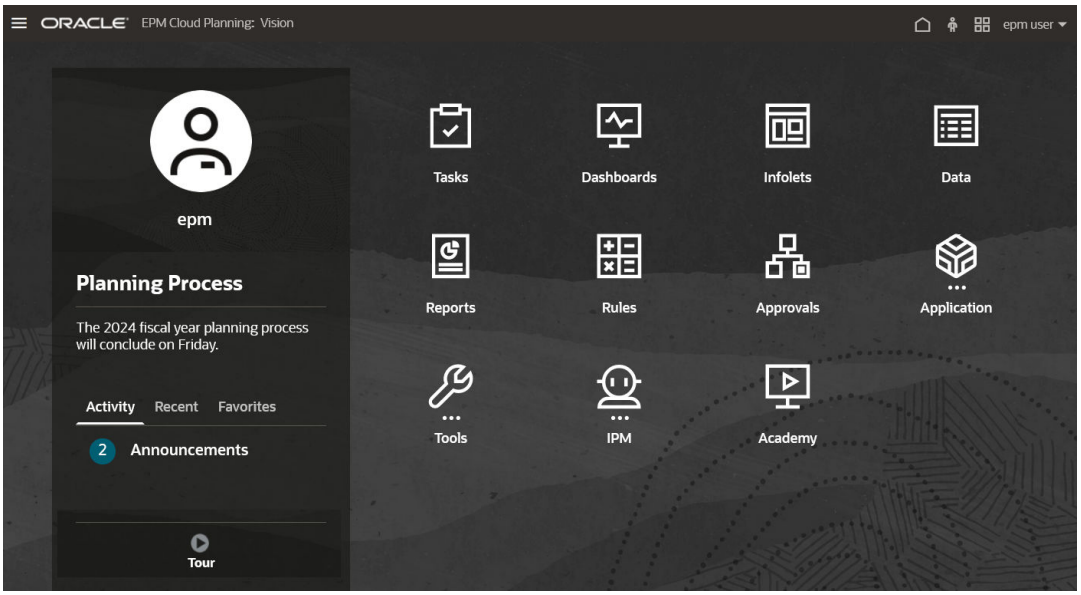
The following themes are available:

- **Oracle** : Features a black global header strip and white home icons. This is the default theme for all new subscriptions.

- **Custom Light :** Features a solid white global header strip with a white background and black icons.



- **Custom Dark** - Features a dark global header and background with white icons.



Logo and Background Image Requirements

For the logo and background image files, select a file of type `.jpg`, `.png`, or `.gif`. The maximum file size is 5 MB.

- **Logo Image**: To avoid distortion, the logo image must be 113 pixels by 32 pixels or an equivalent ratio.
- **Background Image**: The default size for the background image is 1024x768. If you use a larger background image, the image is scaled to fit the resolution setting of your display. If you want your background image to fit both a browser and a mobile device, Oracle

recommends that you size the image so that it fits your biggest screen (or highest resolution device). The background image is centered horizontally.

> **Note**
>
> When switching to a new theme, customers using a custom background image might need to ensure that the color contrast for icons and labels is appropriate. To remedy, consider choosing a different theme or a suitable background.

Understanding Feature Updates

Generally, Oracle releases a patch containing bug fixes, code optimization, and feature updates on the first Friday of the month. Oracle applies this patch to the test environment of the service during the next Daily Maintenance window following a patch release. Typically, production environments are patched on the third Friday of the month.

Monthly Updates to Environments

Oracle notifies Service Administrators of the updates included in each patch. For minor patch releases, Oracle typically provides one week advance notification before patching the test environment. For major updates, Oracle provides a two-month advance notification.

Viewing Readiness Information

A document that provides detailed information about the currently installed service update is posted on the Oracle Cloud Release Readiness website. Information that may be available at this website includes announcements and new features, changes in behavior, and fixed defects.

> **Note**
>
> You can open the Oracle Cloud Release Readiness website directly by going to https://cloud.oracle.com/saas/readiness/overview.

To access readiness information from the service:

1. Access an environment. See Accessing Cloud EPM and Cloud EDM Environments.
2. On the Home page, access **Settings and Actions** by clicking your user name at the top right corner of the screen.
3. Select **About** and then **Version**.
4. Click the **Oracle Enterprise Performance Management Release Readiness** link. Oracle Cloud Release Readiness website is displayed.
5. Click **Enterprise Performance Management**, and then the service type, for example, Planning & Budgeting.

Troubleshooting

Dealing with Down Environments in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Managing Daily Maintenance

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments require daily maintenance. Service Administrators can select (and change) the most convenient time to start the maintenance process.

> **Note**
>
> In Profitability and Cost Management and Enterprise Data Management environment, users with the Migrations - Administer role can also view and change the daily maintenance start time.

In this section:

Daily Maintenance Operations

Every day, during the operational maintenance of the environment, Oracle does the following:

- Create maintenance snapshot called `Artifact Snapshot` of existing artifacts and data. See Backing Up and Restoring an Environment Using the Maintenance Snapshot.
- Apply any required patches (for example, monthly updates, weekly patches, one-off patches)
- Adjust configurations, such as caches
- Analyze all the activities performed and logs created during the last 24 hours and create the Activity Report

Following this, the environment is rebooted, with initial access only to Service Administrators as the maintenance process continues with database backup.

Unavailable Operations During Daily Maintenance

The following table lists the operations that are unavailable when the environment gets restarted and maps them with business processes:

> **Note**
>
> During this period, Enterprise Data Management business has all operations restricted, while specific operations are limited for other processes.

Business Processes	Unavailable Operations
Account Reconciliation	All import and data integration operations

Business Processes	Unavailable Operations
Planning	• Clear Cube • Compact Outline • Data Integration • Export Data • Export Metadata • Import Data • Import Metadata • Merge Data Slices • Optimize Aggregation • Refresh Database • Restructure Cube
Enterprise Profitability and Cost Management	• Clear Cube • Compact Outline • Data Integration • Export Data • Export Metadata • Import Data • Import Metadata • Merge Data Slices • Optimize Aggregation • Refresh Database
Financial Consolidation and Close	• Data Integration • Export Data • Export Metadata • Import Data • Import Metadata • Refresh Database • Restructure Cube
Narrative Reporting	None
Profitability and Cost Management	• Application - Calculation Rules • Application - Dimension Management • Dashboards • Data Integration • Import Snapshot • Intelligence - Analysis Views • Models - Designer • Models - Execution Control
Tax Reporting	• Data Integration • Export Data • Export Metadata • Import Data • Import Metadata • Refresh Database • Restructure Cube

> **Note**
>
> - Operations for Planning, Enterprise Profitability and Cost Management, Financial Consolidation and Close, and Tax Reporting are restricted during Daily Maintenance, if invoked through EPM Automate or REST API or scheduled through Job Console. They can be invoked manually from the Job Console, if the user can login.
> - Nothing is completely blocked for Profitability and Cost Management during the entire daily maintenance duration. These operations are blocked partially.
>   - Dimension Management, Dashboards, and Analysis Views are temporarily blocked for a few seconds to over 30 minutes (depending on the dimension members in the application), immediately after the service restarts.
>   - Calculation Rules, Designer, and Execution Control are blocked after the above operations are available, for a few seconds to potentially an hour, depending on the number of rules in the application. Notably, during this duration, Rule operations (such as Designer, Calculation, etc.) become incrementally available based on the specific POV requested by the application.
>   - Import snapshot is blocked during the time the backup is being performed.

Default Maintenance Start Time

Because environments are not available to users during the maintenance window, the Service Administrator should identify a one-hour period when no one uses the service. Any connected user will be logged off and unsaved data will be lost.
The default maintenance start time is between 10:00 p.m. and 1:00 a.m. local time of the region that hosts your environment. If you do not reset the default start time for an environment, Oracle randomizes it to start between 10:00 p.m. and 1:00 a.m. local time of the region. After you select a maintenance start time, Oracle honors your selection. See Setting the Maintenance Start Time for an Environment.

Some services may perform additional maintenance operations. For example, Planning Modules, Account Reconciliation, and Financial Consolidation and Close may require additional maintenance time for content upgrade.

> **Note**
>
> To allow users to save data, Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management display a notice of impending maintenance 15 minutes before the maintenance process starts.

Inform Users of Daily Maintenance Completion

Though a period of one hour is marked for Daily Maintenance, it usually takes much lesser time to complete. You can use a custom script to inform users that daily maintenance is complete so that they can resume their activities. See Inform Users of Daily Maintenance Completion in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*.

Setting the Maintenance Start Time for an Environment

Maintenance start time is set separately for the test and production environments. To set the maintenance start time:

1. Access an environment. See Accessing Cloud EPM and Cloud EDM Environments. You can sign in as a Service Administrator, or as a user with Migrations - Administer application role.
2. Click **Tools** and then **Daily Maintenance**.
   Narrative Reporting only: Click **Daily Maintenance**.
3. Select the time zone of your choice.
4. In **Start Time**, select the time when the maintenance process should start.
   The maintenance of the environment need not start at the top of the hour. You can set the hour and the minute for the daily maintenance start time. For example, you can set Start Time to 2:24 pm UTC (14.24 on a 24-hour clock). By distributing the daily maintenance start time throughout the hour, you help reduce the daily maintenance load on the infrastructure.
5. Click **Apply**.

Related Information:

- setDailyMaintenanceStartTime in *Working with EPM Automate*
- Setting the Daily Maintenance Time in *REST API for Enterprise Performance Management Cloud*

Scheduling Content Update Start Time

In Oracle Fusion Cloud Enterprise Performance Management, certain business processes require a content update to incorporate the changes made during the daily maintenance of the environment.

What is Content Update?

Content update propagates the changes introduced during the daily maintenance of an environment. If a content update is required, Oracle creates and schedules a content update job, which will, by default, be executed 3 hours after the daily maintenance is completed. All activities in the environment are suspended while content update is in progress.

If other jobs are active in the environment when the content update job is scheduled to start, the content update job will wait for upto three hours before being rescheduled for the next day. If a similar situation prevails the next day, the content update is forcibly executed during the next scheduled daily maintenance.

> **Note**
>
> Self-service content update is supported only for Planning Modules, Sales Planning, and Strategic Workforce Planning. Content update for Financial Consolidation and Close and Tax Reporting business processes is performed immediately after completing daily maintenance.

Determine the Content Update Start Time

Service Administrators can control the start time of content update processes by specifying an offset relative to the daily maintenance start time. You can schedule the update to begin any time within a 1 to 12 hour window after the daily maintenance starts. The maximum deferral for the content update is 12 hours, and Oracle will create and schedule the content update job based on your selected settings.

If the content update fails to complete, it will automatically be triggered after the next daily maintenance, bypassing the scheduled time.

If content update fails at any stage, the application enters the administration mode, and only Service Administrator can access it. For example, Oracle performs a cube refresh after the content update, which may fail because of application customizations such as incomplete changes to the outline or metadata that were introduced during the content update. The cause of the failure can be determined by checking the status of the **Content Update** job. See Handling Pre-Validation Errors.

To solve the failure, Service Administrator can:

- Sign into the environment and manually remove or finish the updates that caused the failure
- Run one or more REST APIs to remove or finish the updates that caused the failure
- Run one or more EPM Automate commands to remove or finish the updates that caused the failure

If a Service Administrator signs into an environment for which content update is scheduled, a screen indicating the scheduled content update is displayed. From this screen, the Service Administrator can start the content update or schedule it for later.

Scheduling Content Update

To schedule content update:

1. Access an environment as a Service Administrator, or a user with Migrations- Administer role. See Accessing Cloud EPM and Cloud EDM Environments.
2. Click **Tools**, then **Daily Maintenance**, and then **Content update scheduling options**.
3. Using **Hours** and **Mins** drop down lists, select the offset time for starting the update. This offset is in relation to the daily maintenance start time.
   If daily maintenance is in progress at the content update start time, the environment will wait for the maintenance process to end before starting content update.
4. To always start the content update at the default update start time, select **In the future, automatically update the application content**.
5. Click **Save**.

Handling Pre-Validation Errors

In case the scheduled content update fails, you will get the following pre-validation error message:

```
Update of the application content could not start because metadata changes were made and successful cube refresh was not run (but no data is lost)
```

To view pre-validation errors or check the progress of a content update:

1. On the Home page, click **Application**.
2. Select **Jobs**, then click **Schedule Jobs**.
3. Use the filter options to narrow down your search.
4. From the **Job Type** dropdown, select **Content Update.**
5. Apply any additional filters as needed, then click **Apply**.

To resolve pre-validation errors and update content:

1. Review the job details to identify the corrective actions needed based on the error message.
2. After addressing the issues, return to **Content update scheduling options** screen, run a successful cube refresh, and then click **Update Now** to start the content update.

To postpone the content update until the next maintenance window, click **Skip**. This will return you to the Home page, and the content update will be rescheduled for the next available maintenance window.

Troubleshooting

See Managing Content Update Issues in *Oracle Enterprise Performance Management Cloud Operations Guide.*

Helping Oracle Collect Diagnostic Information Using the Provide Feedback Utility

Use the Provide Feedback utility to help Oracle diagnose and resolve issues efficiently. This utility is available within the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

If you encounter an issue while using the service, use the Provide Feedback utility to describe the issue and the steps to reproduce it. To expedite the resolution of issues, Oracle recommends that you add multiple screenshots to your feedback submissions. Adding a succession of screenshots that show your progress through a task enables you to create a storyboard that shows Oracle how to recreate your issue.

Each time a user submits feedback to Oracle using the Provide Feedback utility, a feedback notification, a subset of the information that a user submits, is sent to Service Administrators and to the user who submits the feedback. These notifications enable Service Administrators to review submitted issues and suggest corrective actions. Feedback notification is enabled by default.

Each Service Administrator can turn off the notification by clicking the **Unsubscribe** link embedded in the email. See Disabling Feedback Notification. Regardless of the subscription status, a notification is always sent to the user who submits the feedback.

You can also provide feedback (text only) to Oracle using the feedback EPM Automate command if the user interface becomes unresponsive.

Your Goal	Learn How
Understand the information that you need to submit to quickly resolve issues	 Overview Video
Understand the process of collecting and submitting information using Provide Feedback	 Overview Video

Key Considerations Before Submitting Application Snapshots

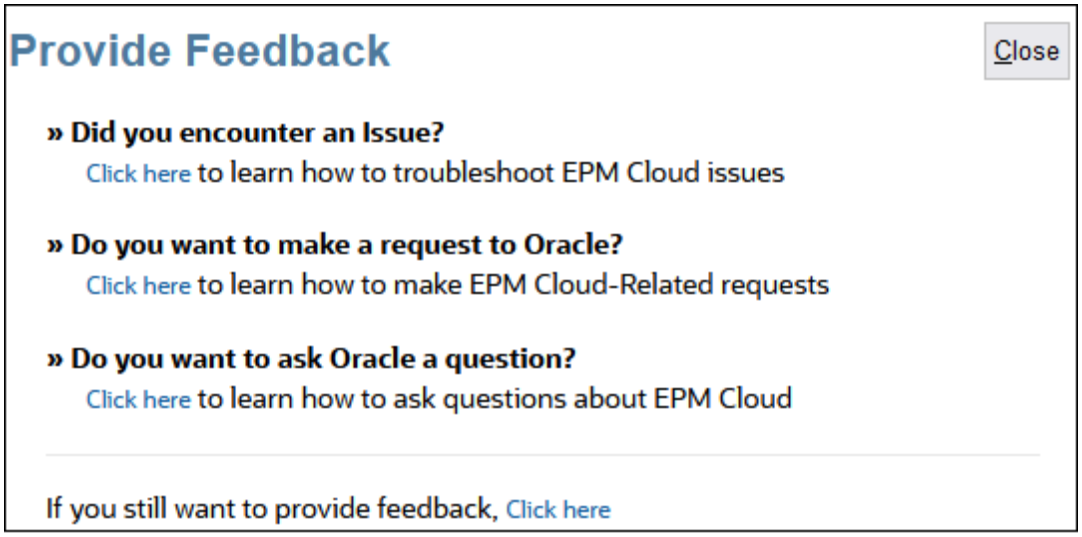
In all non-restricted OCI regions, Service Administrators can choose to consent to submit the last maintenance snapshot of the environment to Oracle when providing feedback. If you agree to submit the maintenance snapshot, Oracle will automatically encrypt and copy the current maintenance snapshot. Oracle uses the submitted application snapshot solely for testing purposes; with no change to the application or data. Before submitting feedback, ensure you are at the point in the process where the problem was observed.

- If your organization enforces a policy that restricts data access by Oracle, you can prevent Service Administrator from submitting application snapshot to Oracle. To do so, set the restricted data access to true using the following EPM Automate command or REST API:
  - Set Restricted Data Access in *REST API for Enterprise Performance Management Cloud*
  - setRestrictedDataAccess in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*

  Once you have set the data restriction, the **Submit application snapshot** check box in the Provide Feedback utility will be greyed out.
- The snapshot submitted to Oracle is the one created by the last daily maintenance. If you want to submit the latest snapshot that has all the changes done since the last daily maintenance, before submitting Provide Feedback:
  - Change the time of the daily maintenance to start at the next hour
  - You can also run `runDailyMaintenance` EPM Automate command, and create a new snapshot before submitting Provide Feedback. See runDailyMaintenance in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- It is your responsibility to keep backup copies of the maintenance snapshot for recovery purposes. Oracle cannot restore your service using the snapshot that you submit. See Backing Up and Restoring an Environment Using the Maintenance Snapshot
- Using the Provide Feedback utility to submit diagnostic information sends your submission to Oracle but does not create a service request. If a Service Administrator cannot resolve the issue, then you can create a service request using the information that you submit. While creating the service request, you are prompted for the reference number, which is displayed on the screen when you submitted diagnostic information using the utility. Additionally, the reference number is included in the feedback notification email. Entering the reference information helps Oracle to easily collect the required diagnostic data.

Submitting Information Using Provide Feedback

1. While you are in the screen about which you want to provide feedback, access the Provide Feedback utility using one of these options.
   - Click your user name (displayed at the right top corner of the screen), and then select **Provide Feedback**.
   - **For Oracle Fusion Cloud Enterprise Data Management and business processes other than Enterprise Data Management:** If you are in an Access Control or Migration modal window, click  (User Assistance) and then select **Provide Feedback**.
2. **Provide Feedback** lists links to self-learn how to resolve specific issues. If you still want to provide feedback, click the link at the bottom.



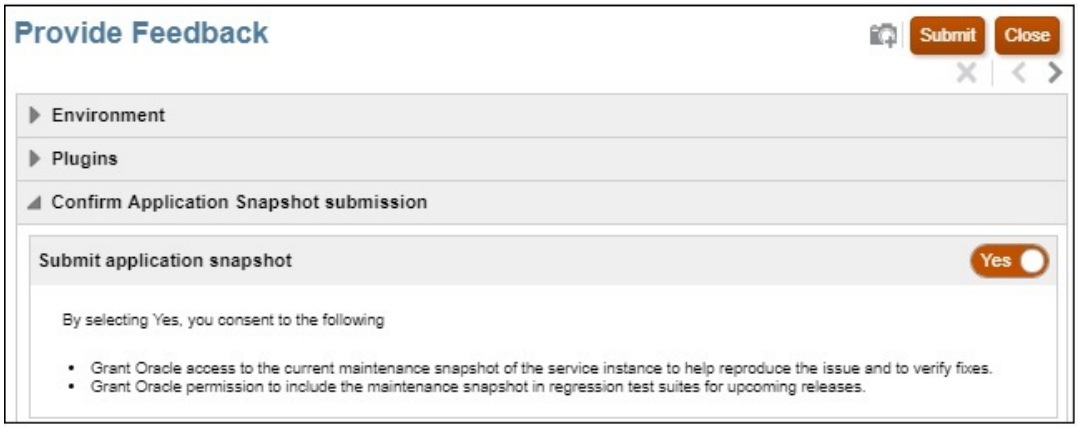
3. **Mandatory:** In **Give a brief description**, describe the issue that you encountered.
4. **Optional**: Select an option to highlight or darken areas of the screen.
   - Select **Highlight**, and then click and drag on the screen to highlight portions of the screen; for example, to highlight errors or issues.
   - Select **Darken**, and then click and drag on the screen to hide portions of the screen. Use this option to hide sensitive data from the screenshot.
5. Click (Add button) to capture the screenshot.
6. **Optional:** Add additional screenshots:
   a. Navigate to the new screen that you want to capture.
   b. Click (Add).
   c. **Optional:** Select an option to highlight or darken areas of the screen, and then click and drag on the screen to highlight or darken an area.
   d. Describe your issue or the actions that you performed in the current screen.
   e. Click **Add**.
   f. Repeat these steps to add more screenshots.
7. Click **Submit**.
8. Review the **Environment** and **Plugins** information.
9. Click (Next) to review screenshots.
10. **Optional:** You may allow Oracle to access the maintenance snapshot. Click **Confirm Application Snapshot submission**.

> **Note**
>
> This option is disabled if your organization enforces a policy that restricts Oracle's access to data, preventing Service Administrators from submitting the application snapshot to Oracle. It is also disabled in all restricted OCI regions (for example, regions in the OC2 and OC4 realms).

11. If **Submit application snapshot** is greyed out and you click it, you get this error message:

    `Service Administrator has restricted data access to Oracle. Thus, the application snapshot cannot be submitted with Provide Feedback.`

12. If **Submit application snapshot** is enabled, choose **Yes** option.



13. Click **Submit**.
14. **Optional**: If you need Oracle's assistance to resolve this issue, follow the instructions on the screen to log a service request. While creating the service request, be sure to enter the **Reference Number** that is displayed on the screen. The reference number is included in the feedback notification email also.
15. Click **Close**.

Disabling Feedback Notification

By default, Service Administrators get a feedback notification each time a user submits feedback to Oracle. Each recipient can unsubscribe from the notification mailing list.

Service Administrators use the information included in the notification to review the issue and suggest corrective actions.

If you unsubscribe, feedback notification are disabled for you after the next daily maintenance of the environment. You will, however, continue to receive notification of any feedback that you submit.

> **Note**
>
> If you disable feedback notification, you cannot enable it again.

To disable feedback notification:

1. Open the feedback notification email (sent by `EPM Cloud User Feedback`), and then click **Unsubscribe**.
2. Sign in to the environment if prompted.
3. Click **Unsubscribe**.
4. Click **Close**.

Creating a Custom Description for an Environment

Can I Change the Service Name of an Environment?

Each environment in your subscription is assigned a name at the time you create the environment. Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management do not allow you to change these names. See Creating an Environment.

How Can I Distinguish Services with Similar Service Names?

Identifying a specific environment, at times, is difficult if you have many environments with similar names. These are the ways to distinguish the environments:

- Create a custom (vanity) URL for each environment. See "Using Vanity URLs" in Resolving Login Issues.
- Create a unique bookmark for each environment.

Using Vanity URLs

Vanity URLs make it easier to remember the complex URLs for the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. These custom URLs can be used to access the environments via a web browser, Oracle Smart View for Office (20.200 and higher), and EPM Automate. To create a new vanity URL, you can use third party link shorteners (for example, T.ly, Bitly, Rebrandly or TinyUrl) or an open source solution (e.g. YOURLS). If you are using an API gateway or reverse proxy, substitute the environment URL with its URL and the context defined for your environment.

Learn to create a Vanity URL and facilitate a connection with Cloud EPM and Cloud EDM using:

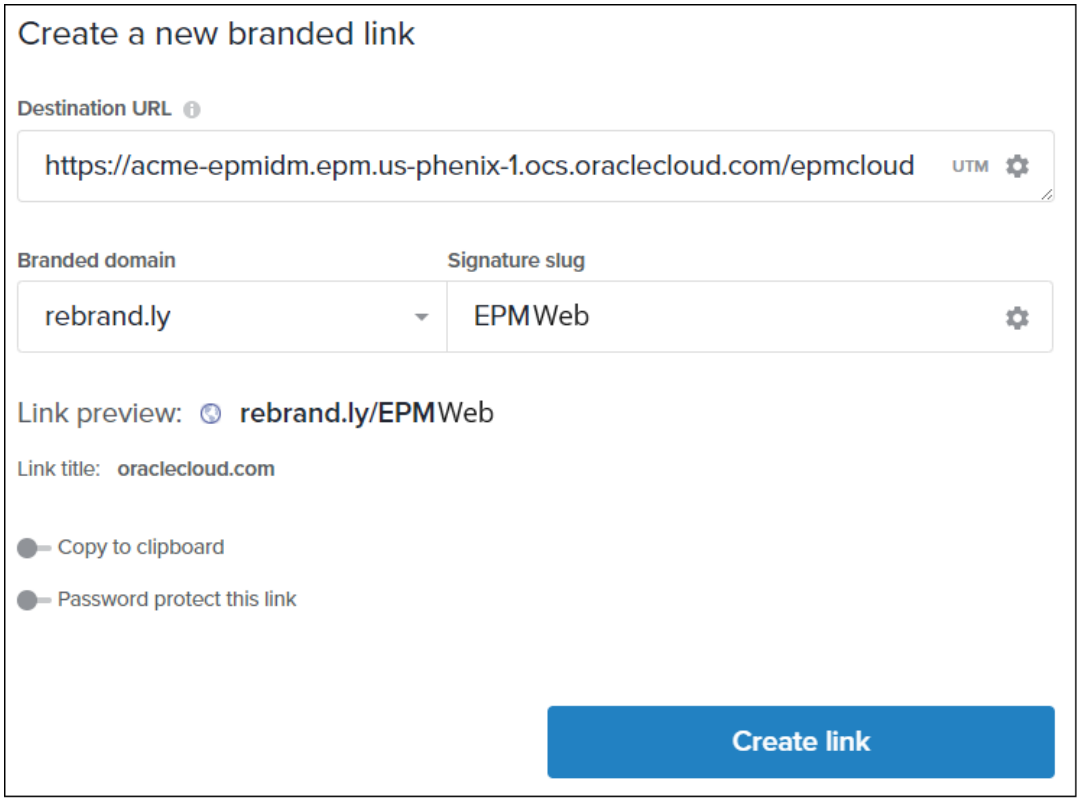
- Web Browser
- Smart View
- EPM Automate

> **Note**
>
> Vanity URLs do not work for cross-environment connections (EPM Connect), and EPM Agent.

Creating a Vanity URL and Connecting Using Web Browser

This example demonstrates how to use Rebrandly to create a Vanity URL.

1. Enter the complete Cloud EPM or Cloud EDM URL in **Destination URL** that you need to simplify with a Vanity URL. Include context `/epmcloud`.
2. Enter a custom URL in **Signature slug.**
   Rebrandly generates a Link preview, showcasing the newly created Vanity URL.
3. Click **Create link** to create this Vanity URL.



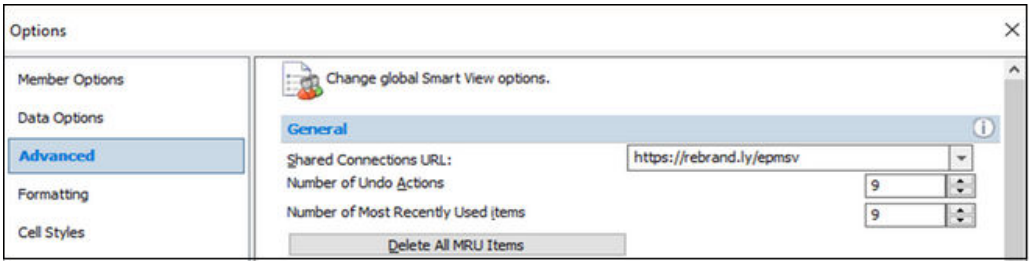
4. Enter the Vanity URL (e.g. `https://rebrand.ly/EPMWeb`) in the web browser to be redirected to the Cloud EPM or Cloud EDM URL.

Creating Vanity URLs and Connecting Using Smart View

Using Rebrandly, this example demonstrates how to facilitate a connection using Vanity URL in Smart View. There are two types of connections in Smart View - Shared and Private. The Cloud EPM and Cloud EDM URLs for both connections follows a specific syntax required for these connections. See URL Syntax for Smart View Connections. You need to create one Vanity URL for Shared connection and another one for Private connection.

Creating a Vanity URL for Shared Connection in Smart View

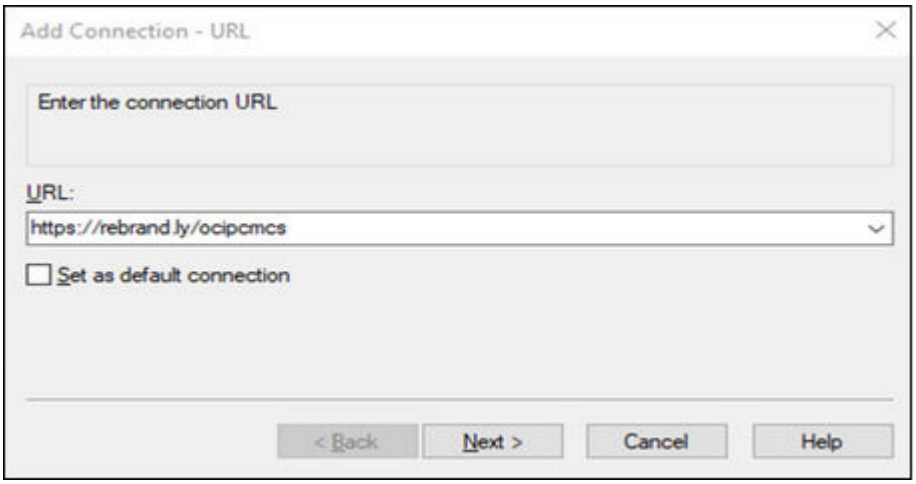
1. Enter the **Destination URL** `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/workspace/SmartViewProviders`.
2. Enter **Signature slug** `epmsv` to create a new Vanity URL `https://rebrand.ly/epmsv`.
3. To facilitate a shared connection in Smart View, follow the steps in Configuring a Shared Connection. For this example:
   a. In **Advanced** settings, add the Vanity URL in **Shared Connection URL**.



b. Click on Shared Connection logon to access the Cloud EPM environment using Smart View.

Creating a Vanity URL for Private Connection in Smart View

1. Enter the **Destination URL** `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com/HyperionPlanning/SmartView`.
2. Enter **Signature slug** `ocipcmcs` to create a new Vanity URL `https://rebrand.ly/ocipcmcs`.
3. Follow the steps in Configuring a Private Connection.
   a. In **Private Connection Wizard**, follow the steps and add the Vanity URL in this step:



   b. Complete the rest of the steps. Click on Private Connection logon to access the Cloud EPM environment using Smart View.

Creating a Vanity URL and Connecting Using EPM Automate

Using Rebrandly, this example demonstrates how to facilitate a connection using Vanity URL with EPM Automate.

1. Enter the **Destination URL** without a context such as `epmcloud` for example, `https://acme-epmidm.epm.us-phoenix-1.ocs.oraclecloud.com`.
2. Enter **Signature slug** `Automate` to create a new Vanity URL `https://rebrand.ly/Automate`.
3. Issue EPM Automate login command using this Vanity URL.

```
Microsoft Windows [Version 10.0.22631.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\example>cd "c:\Oracle\EPM Automate"\bin

c:\Oracle\EPM Automate\bin>epmautomate login example@example.com examplepwd https://rebrand.ly/Automate
```

Understanding Encryption Levels

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management uses Transport Layer Security (TLS) with strong ciphers to secure communication and data. Currently, Cloud EPM and Cloud EDM do not support mutual TLS (mTLS) authentication.

Browsers, Smart View, and EPM Automate

Cloud EPM and Cloud EDM use Transport Layer Security (TLS) with strong ciphers to secure communication with browsers, Oracle Smart View for Office, and EPM Automate.

Oracle recommends that you install the newest version of the supported browser. Generally, the newest version is compatible with higher cipher strengths and has improved security. See Supported Browsers.

SAML Messages to Identity Providers

- Oracle Access Manager, which is the default Service Provider (SP), uses the MD5 algorithm to sign SAML messages to the Identity Provider (IdP) that you configured when setting up SSO. See Configuring Security Settings.
- If your IdP, for example, SiteMinder, indicates that the signature validation of authentication request from the SP fails because it is signed using MD5 while the IdP supports only newer algorithms (such as RSA), create a service request containing an Exception Request asking Oracle to provide SSO SP XML metadata (in SHA-256 format). In the service request, indicate `Hosting Services` Problem Type.
- On receiving the service request, Oracle will attach the SP metadata in SHA-256 format to the service request, which you can extract and upload to the IdP.
- Cloud EPM and Cloud EDM relational data is encrypted using Transparent Data Encryption (TDE).

Navigation Flows and Connections

The credentials and other secure parameters used in Navigation Flows and Connections are encrypted using AES-256.

Session Management

To ensure security, Cloud EPM and Cloud EDM encrypts all sessions. The session information contained in cookies is encrypted and the session ID is randomly generated.

Changing Idle Session Timeout Settings

Idle Session Timeout defines the period of user inactivity after which a session is automatically terminated, and the user is signed out of the identity domain.

The timeout settings can be configured at two-levels:

- **Identity domain level** - Applies to all environments within the domain.
  Default value: 480 minutes. To change this setting, see Changing the Session Time-Out in *OCI documentation*.
- **Individual environment level** - Applies only to a specific Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environment.

Default value: 75 minutes (configurable between 4 and 480 minutes). To change the environment-level timeout, use one of the following:

- EPM Automate command - setIdleSessionTimeout in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- REST API - Set Idle Session Timeout in *REST API for Enterprise Performance Management Cloud*

> **Note**
>
> - The **effective idle session timeout** for an environment is the shorter of the value set at the identity domain level or individual environment level. Once a session remains idle for the effective timeout duration, the user is automatically redirected to the login page.
> - In addition to idle timeout, environments also enforce a **maximum session duration**. Regardless of activity, users are logged out once the maximum duration is reached.. See Maximum Session Duration.

Sender Email Address

The default sender email address for the emails sent from Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments is no.reply@epm.oraclecloud.com. You can also request outgoing messages to use custom sender email address, see Request Custom Sender Email Address for OCI (Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide* .

Configuring SPF Record for Email Verification

Oracle publishes the Sender Protection Framework (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.

If your environments are located in	Add this to the SPF record
Americas	`v=spf1 include:rp.oracleemaildelivery.com ~all`
Asia/ Pacific	`v=spf1 include:ap.rp.oracleemaildelivery.com ~all`
Europe	`v=spf1 include:eu.rp.oracleemaildelivery.com ~all`
All Commercial Regions	`v=spf1 include:rp.oracleemaildelivery.com include:ap.rp.oracleemaildelivery.com include:eu.rp.oracleemaildelivery.com ~all`

DKIM Support

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments support DKIM (DomainKeys Identified Mail). The

email servers sign outgoing messages with a private key, allowing receiving mail servers to verify the signatures using a public key published in the `oraclecloud.com` DNS record.

> **Note**
>
> Oracle's support for DKIM works for emails where the domain address is `no.reply@epm.oraclecloud.com` or a custom email address. To request outgoing messages to use custom sender email address, see Request Custom Sender Email Address for OCI (Gen 2) Environments in *Oracle Enterprise Performance Management Cloud Operations Guide* .

Get DKIM Selector Value

To find the DKIM public key from `oraclecloud.com` DNS record, use the `DKIM Selector` value referenced in the header information sent in the email. DKIM selector is referenced by `header.s=` *VALUE* where `header.d` is `oracle.cloud.com`.

For example, in the following header information of an email from sender domain `no.reply@epm.oraclecloud.com`:

```
Authentication-Results: ppops.net;
spf=pass
smptp.mailfrom=bounces+jane.doe=oracle.com@server.rp.exampleleemaildelivery.co
m;
dkim=pass header.s=emaildelivery header.d=oracle.cloud.com;
dkim=pass header.s=ACCOUNT_NAME header.d=server.rp.oracleemaildelivery.com;
dmarc=pass header.from=oracle.cloud.com
```

DKIM selector value is `emaildelivery`.

Get Public Key

Using the DKIM Selector value (for example, `emaildelivery`) and the sender domain `no.reply@epm.oraclecloud.com`, get the public key in the following ways:

- Check DNS-related records from a website, for example `https://www.mail-tester.com/spf-dkim-check`.
- Run the following command on Linux/ MAC OS command line:

  ```
  dig domainSelectorValue._domainkey.oraclecloud.com TXT +short
  ```

Using the methods above, here is the public key for the DNS record for `emaildelivery._domainkey.oraclecloud.co`:

```
"k=rsa\;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9Td5RdIXZ9SC4q49SCnB+iR7
/TCmlnvu/54GMARLiik6lkF+h0C+Ek8z2UfPU3J/Nj+Rt+Q9Dvuvpdfzw/vfwE1yT4/
ZdncRNzQ+rI5NfC6oi4F6X3ZpZ3sx0pu6TwAoJszeVzQTHS4xt4EhGeM"
"hSaKMWTO23H7/5/4/7Je3zbt0VsPJ3zXArOOLiBS7TuN3RUAVh4CPDbmP2Ddzr6GWOkUzJq+lPH8t
ybOb/6jv5He2vVt35r/
VUXEaotvQzo7h8eLTOe8AgmyCDYeLPOTWoPSiZ7KdJW0Cly5eP8WZJaT2beBeUzBB7x1q7a/
vt5f4YwllcD8VC+zeK/64BSLQ5wIDAQAB"
```

Key length : 2048

Retrieving Data After Service Termination

Data from terminated Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments is available to you for a period of 60 days.

11

Integrating Cloud EPM and Cloud EDM with Oracle Guided Learning

Oracle Guided Learning (OGL) offers a robust framework for developing personalized, guided, and contextual training and user onboarding experiences. Beyond the EPM documentation, this versatile toolset includes the options to create custom process guides, display groups, message guides, smart tips, and more. It offers a comprehensive learning interface tailored to meet specific needs within Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments, enhancing user proficiency and operational efficiency. For a detailed overview, see Introduction & Overview of Oracle Guided Learning in *Oracle Guided Learning User Guide*.

The users have access to OGL Console, which allows them to define content that streamlines adoption by enabling them to design and activate in-application guidance tailored to specific workflows and requirements. For instance, you can create OGL guides for your Navigation Flows.

Configuring Settings in the Environment

Before proceeding, ensure you have an active OGL account and at least one Application ID (App ID) set up. An App ID is a logical grouping of guides (contents). Each App ID can group guides customized for EPM workflows for a particular business process. For setup details, see Getting Started in *Oracle Guided Learning User Guide*.

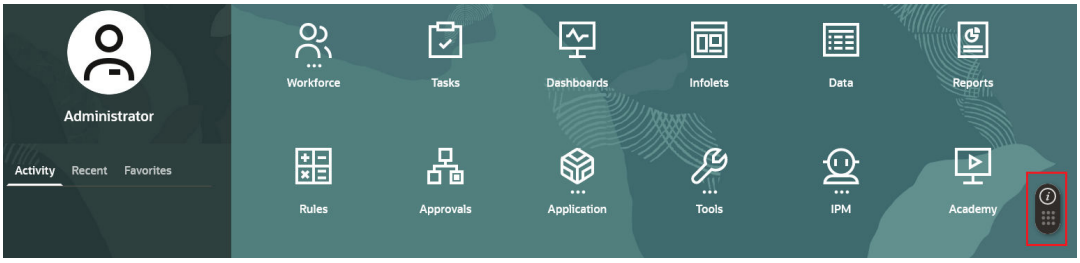
> **Note**
>
> When integrating an OGL App ID to use OGL Help within a Navigation Flow, configure it solely at the source environment. OGL setup is unnecessary on any of the connected environments.

Follow these steps to integrate an OGL application into your environment:

1. Navigate to **Applications**, then **Settings**

   Narrative Reporting and Cloud EDM only: Navigate to **Tools**, then **Settings**

   Account Reconciliation only: Navigate to **Applications**, then **Configuration**, and then **System Settings**
2. Enter the following Oracle Guided Learning Settings:
   - **Application ID**
   - **Server URL** - Depending on the location of your environment, enter the URL:
     - NA: `https://guidedlearning.oracle.com`
     - EMEA: `https://guidedlearning-emea.oracle.com`
     - APAC: `https://guidedlearning-apac.oracle.com`
3. Click **Save**. You'll need to log off and log back in for the OGL widget to display on your screen.



Configuring settings in the OGL Environment

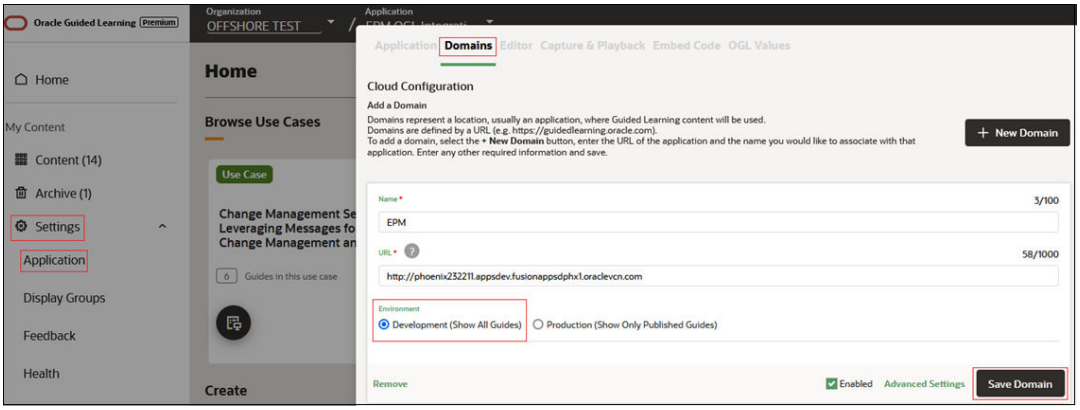
Once the OGL Application is integrated into the Cloud EPM and Cloud EDM environments, the OGL widget will be accessible to the users. Only published guides are visible since the domains by default is configured to Production, which hides the guides that are in development mode.

To allow users to view both published and in-development guides from the environment, change the application's settings as follows:

1. Access the OGL Console application settings. See OGL Console Left Panel in the *Oracle Guided Learning User Guide*.
2. Navigate to the **Domains** tab.
3. Select the **Environment** to **Development** to display all guides.
4. Check the domain status to **Enabled.**

> **Note**
>
> Please make sure to complete the domain entry configuration correctly so that OGL content displays correctly on all applications. Remember OGL content won't appear for domains not listed in OGL Cloud Configuration.

5. Click **Save Domain**.



Key Considerations

- Cloud EPM and Cloud EDM environments are required to perform daily maintenance. Oracle generates a maintenance snapshot, known as an Artifact Snapshot, which captures existing artifacts and data. It's important to note that OGL configuration in Cloud EPM and

Cloud EDM is not integrated, and therefor is not included in the Artifact Snapshot. For more information, see Exporting OGL Guide Content in *Oracle Guided Learning User Guide*.

- If the Cloud EPM and Cloud EDM environments have Network Perimeter setup, the IP address of the OGL server or the outbound IP address of the region that hosts the OGL server must be added to the Network Perimeter. See Outbound IP Addresses of Cloud EPM Data Centers and Regions in *Operations Guide*.

Enabling Context-Based Activation of OGL Guides in Cloud EPM

Oracle Guided Learning (OGL) seamlessly integrates with applications to capture their workflows, enabling precise, in-application guidance tailored to user needs. The **Advanced Setting** feature in the **OGL Editor** further enhances this capability by allowing Service Administrators to:

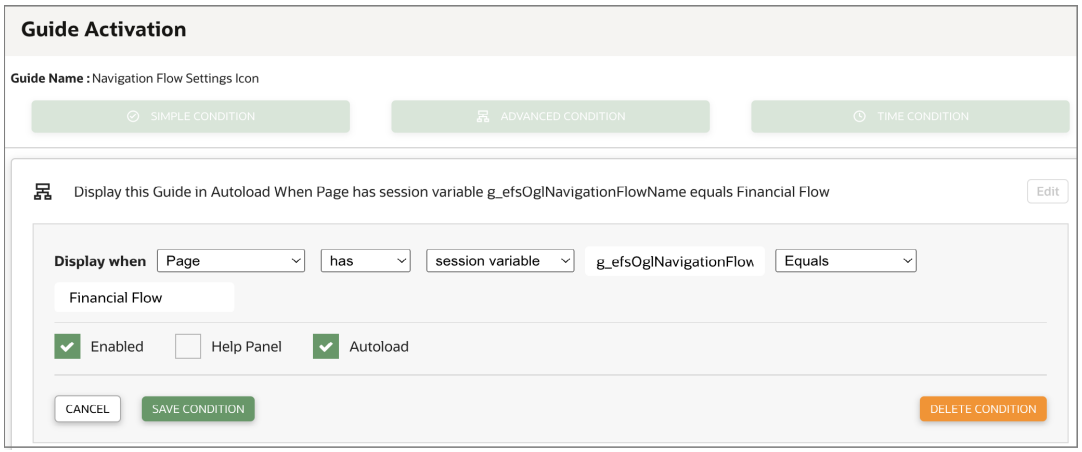
- Configure conditional activation based on Navigation Flow name, cluster ID, card ID, tab, or sub-tab ID.
- Incorporate dynamic content and define custom triggers for guide activation.
- Control visibility and placement of guidance on-screen.

This flexibility ensures that OGL guidance can be fine tuned to meet diverse business requirements within the application environment. Upon integration, Oracle Fusion Cloud Enterprise Performance Management offers the following attributes for activating guides conditionally on pages or components, allowing advanced settings for context-based activation of OGL Guides in the Cloud EPM environments:

Attributes for Context-Based Activation in Cloud EPM

For more information on updating attributes, see Working with the Editors in *Oracle Guided Learning User Guide*.

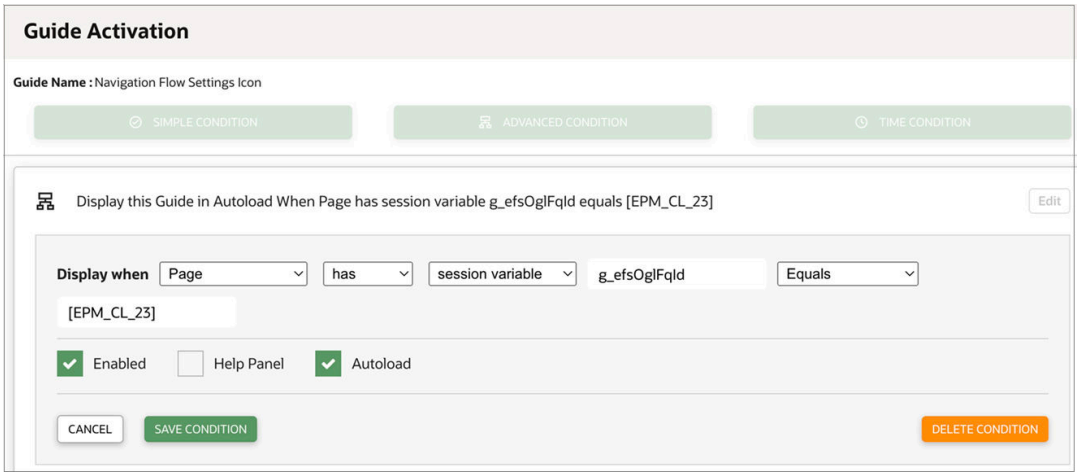
- **Activating Guides by Navigation Flow Name**: Use the attribute `g_efsOglNavigationFlowName` to activate a guide for specific Navigation Flow. For instance, the following condition activates a guide for all pages within the "Financial Flow" Navigation Flow.



- **Activating Guide Names by Page ID:** The attribute `g_efsOglFqId` enables activation at various levels within the navigation hierarchy:
  - `g_efsOglFqId/<SUB_TAB_ID>` - Activates the guide on the specified sub-tab.

- `g_efsOglFqId/<TAB_ID>/<SUB_TAB_ID>>` - Activates the guides on a sub-tab within a specific tab.
- `g_efsOglFqId/<CARD_ID>/<TAB_ID>/<SUB_TAB_ID>` - Activates the guide on a sub-tab within a tab within a specified card.
- `g_efsOglFqId/<TAB_ID>` - Activates the guides for all the pages within the specified tab.
- `g_efsOglFqId/<CARD_ID>` - Activates the guides for all the pages within the specified card.
- `g_efsOglFqId/<CLUSTER_ID>` - Activates the guides for all the pages within the specified cluster.

For instance, the following activation condition for OGL enables a guide for all pages defined in the cluster ID EPM_CL_23.



12

Monitoring the Cloud EPM and Cloud EDM Environments

You use the Activity Report and Access Logs to monitor what is happening in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

Related Topics

- Using the Activity Report
- Activity Report Contents
- Using Access Logs to Monitor Usage
- Viewing and Downloading Activity Reports and Access Logs
- Automating Activity Report and Access Log Download
- Using the Role Assignment Report to Monitor Users
- Monitoring Environments Using Oracle Cloud Console
- Monitoring Metrics

Using the Activity Report

The Activity Report enables Service Administrators to gain deep insights into application usage and associated user experience. By highlighting user requests, calculation scripts, forms, reports, and more, it helps optimize and streamline application design for better performance and efficiency.

Key Benefits

The Activity Report helps you:

- **Understand application usage** by displaying detailed trends in user behavior and system activity.
- **Improve user experience** by identifying operations or requests that impact performance.
- **Spot optimization opportunities** by revealing inefficiencies in usage patterns.
- **Investigate issues quickly** using high-level graphs and detailed tabular reports.
- **Track changes over time** to see how updates affect performance and user behavior.

To fully leverage your Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management environments, combine the Activity Report and other tools to identify trends, troubleshoot issues, and drive continuous improvement.

Report Formats Available

Two versions of the report are available:

- HTML version – easily viewable in a browser

- JSON version – ideal for data analysis, available for download only via the downloadFile EPM Automate command

> **Note**
>
> Activity Reports are only retained for the last **60 days**. Download them regularly to maintain a historical view and support long-term analysis.

Automatically Generating Activity Reports

A new Activity Report is created in the following scenarios:

- During Daily Maintenance of the environment. See Managing Daily Maintenance
- Each time a user submits feedback via the **Provide Feedback** tool (these reports also include screenshots and user-entered descriptions). See Helping Oracle Collect Diagnostic Information Using the Provide Feedback Utility
- Each time the resetService command is executed via EPM Automate

Viewing Activity Report in the Environment

1. Sign in to the environment as a Service Administrator. See Accessing Cloud EPM and Cloud EDM Environments.
2. Click **Application**, then select **Activity Reports** (or **Overview > Activity**).
3. Choose a duration from the **Reports from last** dropdown (**5, 10, 30, or 60 days**).
4. Click on a **report name** to open and review it.

Navigating the Activity Report

Select one of the following tabs for quick access to relevant information:

- **User Interface**: Information about users who accessed the service.
- **Hourly**: Hourly metrics including those on user interface requests and responses and Oracle Essbase operations.
- **Runtime**: Runtime metrics for the application in your environment such as Supplemental Data Manager Active Data Collection Periods or Open Account Reconciliations.
- **Application**: Application design metrics such as Task Manager Org Units or Essbase ASO Cubes.
- **Operational**: Operational Metrics such as Daily Maintenance Duration in minutes.
- **Usage**: Usage by most and least active users.

For more information, see Activity Report Contents.

Activity Report Contents

Depending on the business process from which this report is taken, the statistics of the Activity Report change.

For example, Activity Report taken from Narrative Reporting environments includes the Narrative Reporting Reports and Book statistics. For all other business processes, this report contains Financial Reporting statistics. Service Administrators use these reports to identify

problems faced by users and to compare service usage and performance to those available in a report from the past. Information about these areas is available:

Information About Your Environment

The details regarding the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments found in the Activity Report are outlined in the table below:

Table 12-1 Environment Information Available in the Activity Report

Label	Explanation
Service URL	URL of the environment without any context. For example, `https://env-example-idDomain.dom1.oraclecloud.com`
Data Center	The region that hosts your environment. For example: Data Center : eu-amesterdam-1. To see the list of all OCI regions, see EPM Cloud Data Centers and Regions in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Table 12-1 (Cont.) Environment Information Available in the Activity Report

Label	Explanation
Cloud Infrastructure	Type of infrastructure - OCI (Gen 2): Oracle Gen 2 cloud infrastructure
Identity Domain	Name of the cloud account.
App Type	The business process deployed in the environment. App Types are: • ARCS: Account Reconciliation • EDMCS: Enterprise Data Management • FCCS: Financial Consolidation and Close • Freeform: FreeForm • EPRCS: Narrative Reporting • PBCS: Planning • PBCS (Modules): Planning Modules • PCMCS: Profitability and Cost Management • TRCS: Tax Reporting
Version (Version Status)	Version status of the environment after the last daily maintenance window or after issuing EPM Automate resetService command. See resetService in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*. The following version status is displayed only if the environment is not on the latest monthly update or weekly patch and indicates the reason for it: • **Temporary Config** - Oracle has made a temporary configuration change in the environment. The environment will be merged back in a future monthly update automatically. No customer action is required. • **Update Advancement** – Customer has requested Oracle to apply a monthly update to a production environment prior to the third Friday of the month. The environment will be merged back on the third Friday. No customer action is required. • **Manual Skip Update** - Customer has requested an Upgrade Delay. The environment will be merged back based on when customer has requested it to be merged back. • **One-Off Patch** - Customer has requested a one-off patch. The environment will be merged back when the same fix is in the main line code. • **Skip Update** - Customer has issued a skipUpdate command from EPM Automate or REST API. These are requests that Oracle skip the applying of monthly updates to an environment for a maximum of three consecutive cycles. The environment will be merged back depending on the chosen cycle (in a month, two or three), or when the customer issues skipUpdate remove command. For more details, see: – skipUpdate in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud* – Skip Updates in *REST API for Enterprise Performance Management Cloud*
Oracle Essbase Version	Displays the specific version of the Essbase engine currently used by the environment. See About Essbase in Cloud EPM.
Instance Type	Type of the environment. Instance types are: • Prod: Production environment • Test: Test environment

User Information

User information available in the report includes the following:

- Number of users who accessed the service.
  In addition to the average usage duration for the number of users on a specific day, the report presents information on the number of unique users who logged on each day over the last week, number of unique users over the last seven days, and unique users over the last 30 days.

Number of Users

Metric	10/21	10/22	10/23	10/24	10/25	10/26	Today
Average Duration (Hour:Min)	01:30	01:34	00:00	00:00	01:37	01:37	01:30
Unique Users Count 377	73	77	0	0	73	73	77
Unique Users in Last 30 Days	74	77	73	73	74	77	77
Unique Users in Last 7 Days	73	74	70	70	73	77	74

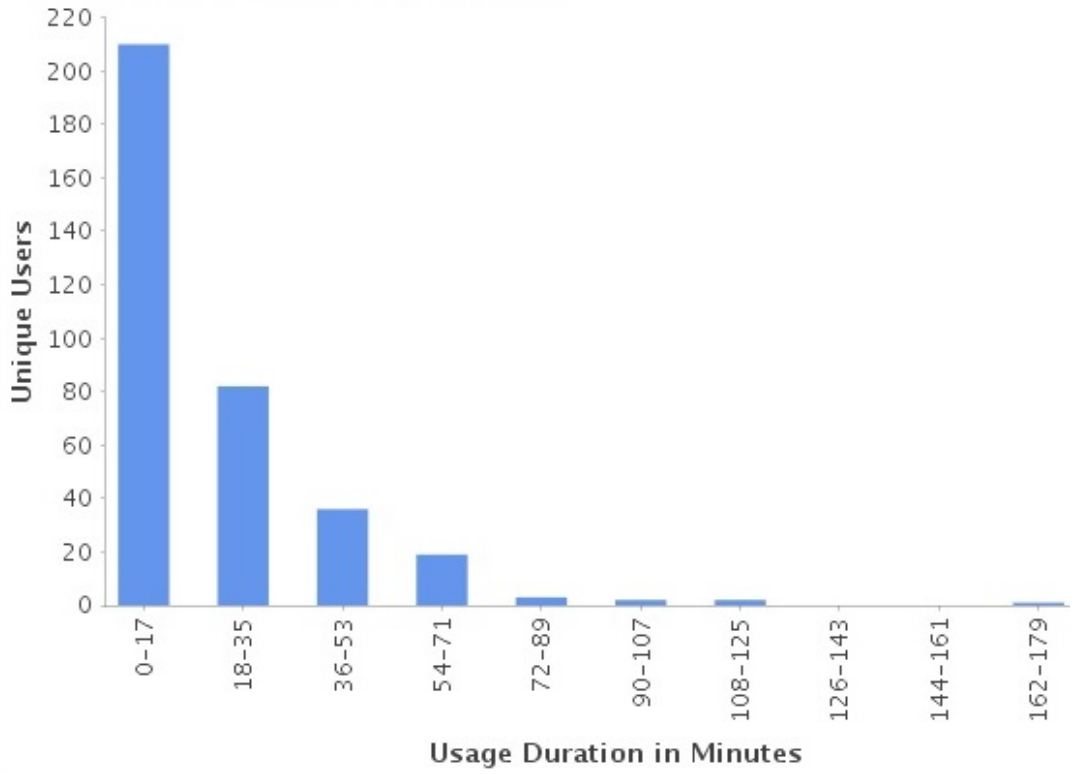
  You can use this information to determine if there is a correlation between the number of users and the performance of your environment.

- List of feedbacks that were submitted to Oracle. This section helps you identify some of the issues that users faced.

User Provided Feedbacks

Time	User	Feedback
17:54:32	janedoe	Feedback submitted in production
17:52:40	janedoe	Feedback submitted in production

- Number of unique users that used the environment for different ranges of durations.



- Top 10 most active users based on usage duration.

Top 10 Most Active Users by Usage Duration

User	Usage Duration (Min:Sec)
user0032	1175:35
user0022	1169:49
user0023	1166:57
user0025	1164:40
user0029	1164:33
user003	1163:30
user002	1162:47
user005	1162:33
user0092	1160:28
user0099	1146:33

- Top 10 least active users based on usage duration.

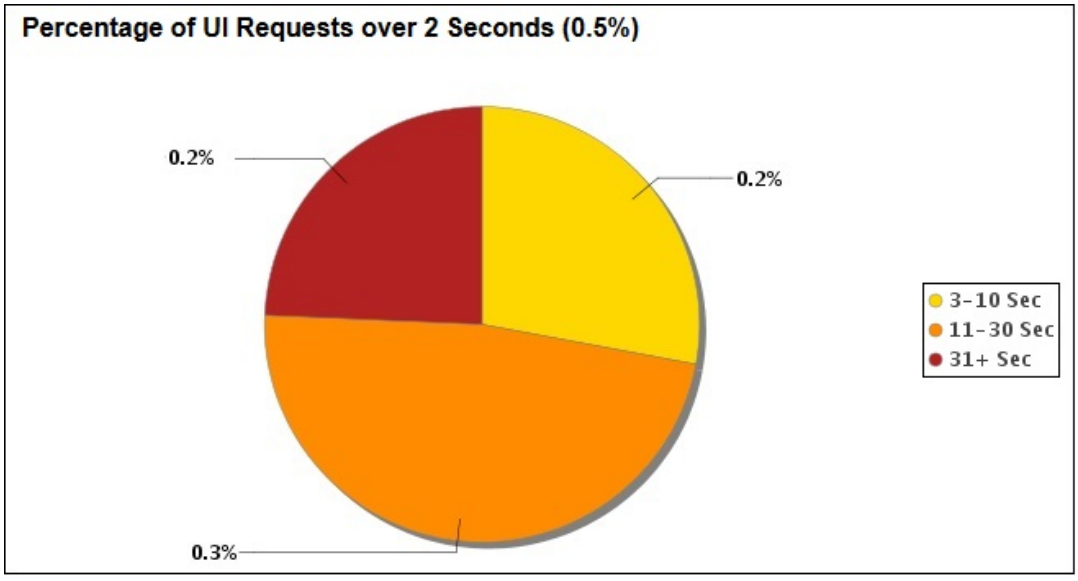
10 Least Active Users by Usage Duration

User	Usage Duration (Min:Sec)
user300	00:00
user200	00:00
user500	04:49
user0092	04:50
user0099	04:58
user0032_1	06:23
user0022_1	06:24
user0023_1	06:24
user0025_1	06:24
user0029_1	06:24

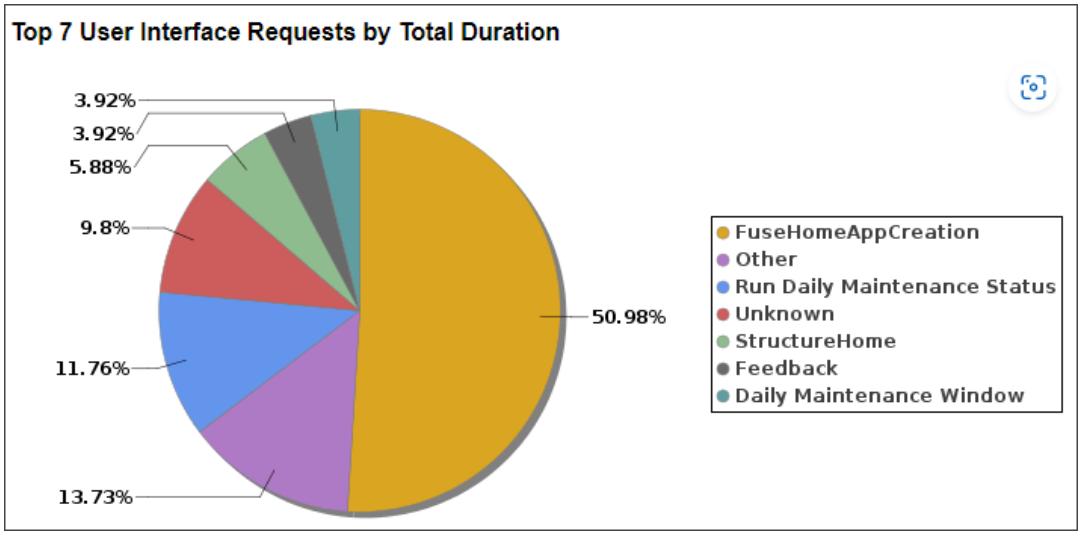
Interface Usage and Response Data

The Activity Report presents the following information on user interface requests and response of the environment:

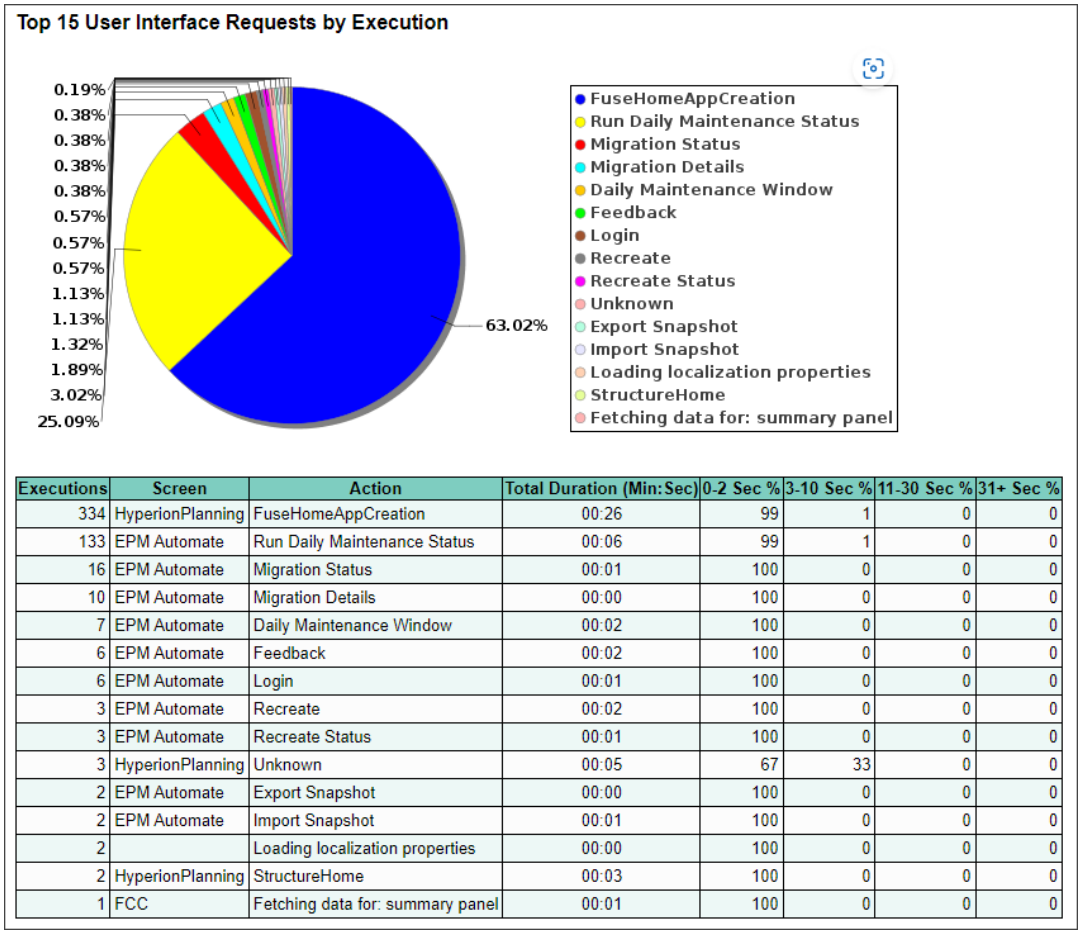
- Percentage of UI requests that took more than 2 seconds to finish.
  A UI request is a user action such as signing in, loading data, opening or saving forms, and validating rules. The section on the top 30 longest running user actions identifies the user, duration of the action, the activity that the user was performing, and the screen that the user was on.



- Top 7 requests that took the most time to complete.



- Top 15 user interface requests that were executed most frequently.



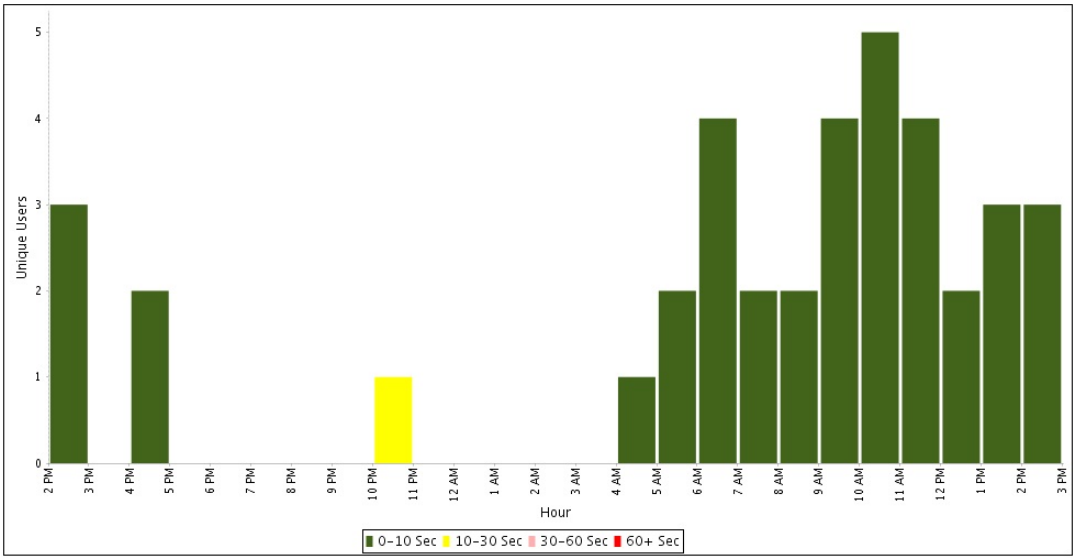
Executions	Screen	Action	Total Duration (Min:Sec)	0-2 Sec %	3-10 Sec %	11-30 Sec %	31+ Sec %
334	HyperionPlanning	FuseHomeAppCreation	00:26	99	1	0	0
133	EPM Automate	Run Daily Maintenance Status	00:06	99	1	0	0
16	EPM Automate	Migration Status	00:01	100	0	0	0
10	EPM Automate	Migration Details	00:00	100	0	0	0
7	EPM Automate	Daily Maintenance Window	00:02	100	0	0	0
6	EPM Automate	Feedback	00:02	100	0	0	0
6	EPM Automate	Login	00:01	100	0	0	0
3	EPM Automate	Recreate	00:02	100	0	0	0
3	EPM Automate	Recreate Status	00:01	100	0	0	0
3	HyperionPlanning	Unknown	00:05	67	33	0	0
2	EPM Automate	Export Snapshot	00:00	100	0	0	0
2	EPM Automate	Import Snapshot	00:01	100	0	0	0
2		Loading localization properties	00:00	100	0	0	0
2	HyperionPlanning	StructureHome	00:03	100	0	0	0
1	FCC	Fetching data for: summary panel	00:01	100	0	0	0

- Top 30 user interface actions that took more than 2 seconds to complete. By analyzing this data, you can identify optimizations that can improve performance.

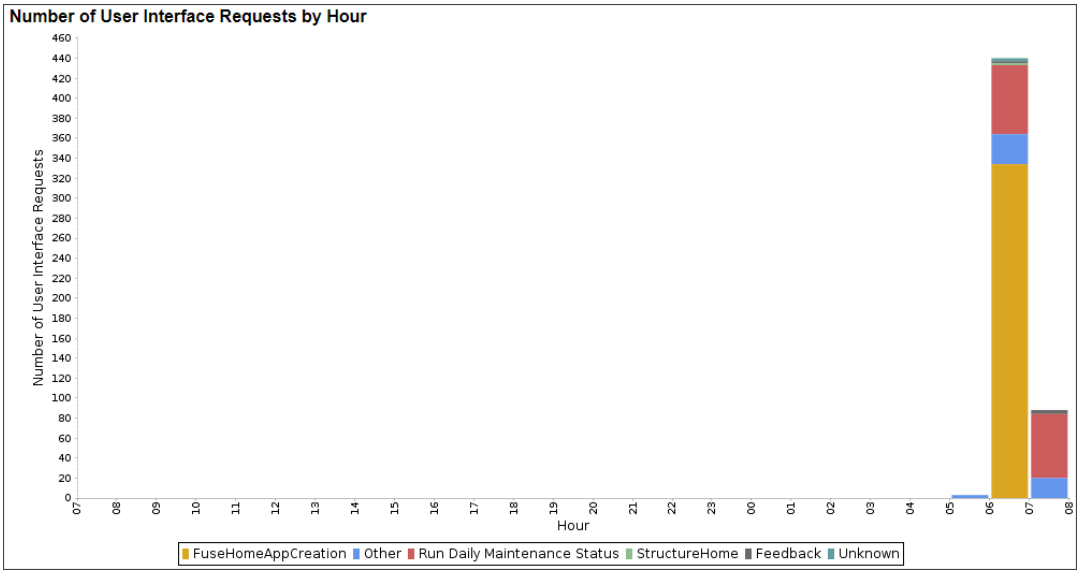
Top 30 Longest Performing User Interface Actions over 2 Seconds

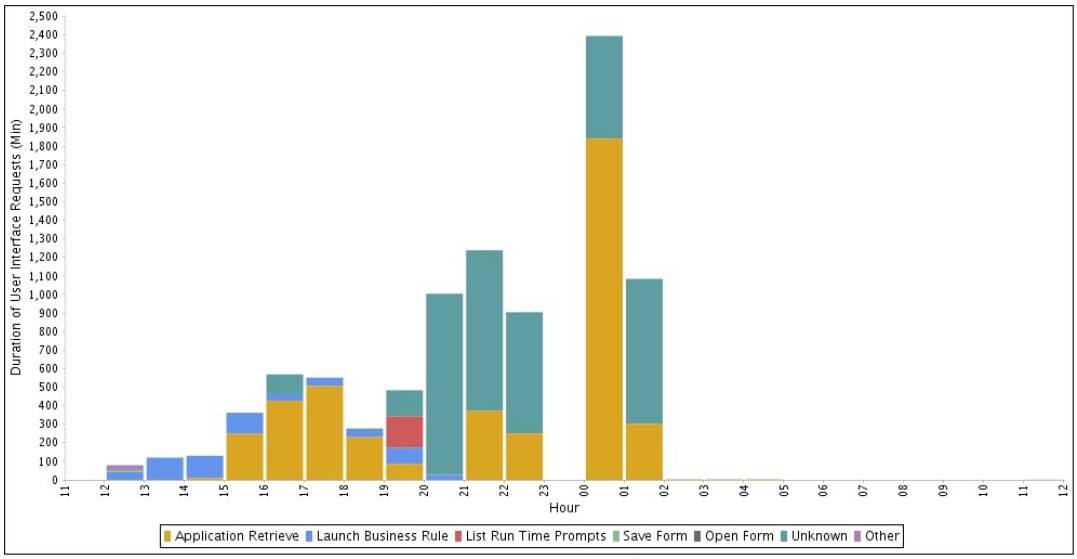
Duration (Min:Sec)	Begin Time	End Time	User	Screen	Action	Parameters	Durations (Min:Sec)
00:05	06:02:28	06:02:33	epmuser	HyperionPlanning	FuseHomeAppCreation		
00:05	06:02:21	06:02:26	epmuser	HyperionPlanning			
00:04	06:03:32	06:03:36	epmuser	HyperionPlanning	FuseHomeAppCreation		
00:04	07:03:52	07:03:56	epmuser	EPM Automate	Run Daily Maintenance Status		
00:03	06:16:55	06:16:58	epmuser	HyperionPlanning	StructureHome		

- Average service response time every hour for the last 24 hours.



- Number and duration of interface requests each hour.





Operational Metrics

The Operational Metrics includes:

Daily Maintenance Duration in Minutes

Duration of how long it takes for Daily maintenance to run in the environment. You can use this information to schedule your jobs outside of the Daily Maintenance window.

Skip Update Requests

Lists the Skip Update Requests currently specified for an environment. These are requests that Oracle skip the applying of monthly updates to an environment for a maximum of three consecutive cycles. Skip updates set for the environment are not listed until after a new Activity Report is generated.

Customer issues a skipUpdate command from EPM Automate or REST API. For more details, see:

- skipUpdate in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Skip Updates in *REST API for Enterprise Performance Management Cloud*

Last Month Availability in Percentage

Lists the percentage of availability of the environment in the last month. It is calculated as the number of minutes the environment was available in the last month divided by the total number of minutes in the last month, converted to a percentage value. For example, if the current month is February 2025, this shows the percentage of availability of the environment in the month of January 2025. If in January 2025, the environment was down for 20 minutes total, the value of this metric will be (44,620/44,640)X100 = 99.96.

Jobs in the Last Hour

This information is available only in an Activity Report generated when a user submits a feedback.

Job Console Records in the Last Hour

Start Time	Duration (Sec)	Name	Type	User Name	Status	Details
18:00:03	354	Content Update	Content Update		Completed	Job updated with parameters: [JOB_ID: 2, PARENT_JOB_ID: -1, SERVER_ID: 1208118367, jobParams: null].
18:00:03	48	Refresh Database	Refresh Database		Completed	Job updated with parameters: [JOB_ID: 3, PARENT_JOB_ID: -1, SERVER_ID: 1208118367, jobParams: {"jobName":"Refresh Database","Security Filters":"false","Update custom-defined functions":"false","Refresh Database":"true"}].
18:04:58	41	Refresh Database	Refresh Database		Completed	Job updated with parameters: [JOB_ID: 4, PARENT_JOB_ID: -1, SERVER_ID: 1208118367, jobParams: {"jobName":"Refresh Database","Security Filters":"false","Update custom-defined functions":"false","Refresh Database":"true"}].

Application Size

This section displays information on the size of the application, including the size of the `Artifact Snapshot`. See Data Size in an Environment for detailed information on data size in Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management.

Table 12-2 Application Size

Metric Name	Description
Customer Data on Disk in GB	Indicates the disk space occupied by a combination of many components. See What Contributes to the Data Size in an Environment?.Size of the data in the relational database is not included in this metric.
Oracle Essbase Data on Disk in GB	Identifies the size of the Essbase artifacts stored on the disk. It includes page files, index files, security files, and so on. For environments that do not use Essbase, for example, Account Reconciliation, this value is 0.
Last Backup Size in GB	Indicates the size of the maintenance snapshot (Artifact Snapshot) created by the most recent daily maintenance process.
Application Management Snapshots in GB	Identifies the size of all snapshots stored in your environment. This includes the size of the maintenance snapshot (Artifact Snapshot) created by the daily maintenance process, all snapshots you exported using EPM Automate or Migration, and all snapshots that you uploaded using EPM Automate or Migration.
LCM Snapshots	Indicates the number of snapshots (including Artifact snapshot) stored in the environment. The size of these snapshots is identified by the Application Management Snapshots in GB metric.
Data Integration Inbox/ Outbox Size in GB	Measures the total amount of data stored in the Data Integration folder. This includes all non-snapshot files that you have uploaded using EPM Automate or Migration.
Size of Data in Database in MB	Indicates the size of the data stored in the relational database.

Application Artifacts

Application Artifacts lists the count of artifacts that you can export from your environment.

To view the list of artifacts for various components in your environment, from the Home page, select **Tools**, then **Migration,** and then **Categories**. See Export Artifacts in *Administering Migration for Oracle Enterprise Performance Management Cloud*.

Examples of Application Artifacts include:

- **Shared Services Artifacts**- Folders, Users, Predefined Groups, Aggregated Roles, Assigned Roles
- **Planning Artifacts**- Application Settings, Service Connection, Year Dimension, Period Dimension, Cube, Plan Type

- **Profitability Artifacts -** Application Data, Dimensions, Preferences, POV, SQL Template Definitions
- **Calculation Manager Artifacts** - Templates, Formulas, Scripts, Rules, RuleSets

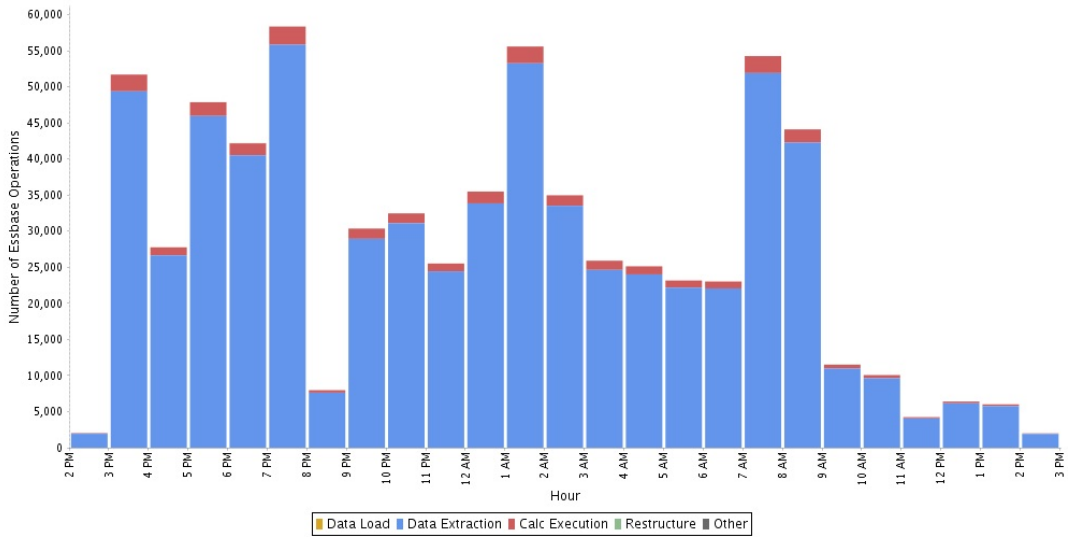
Essbase Statistics

Related Topics

- Essbase Metric
- Essbase Runtime Data
- Essbase Design Metrics and Statistics
- Outline Warnings

Essbase Metric

- Number and Type of Oracle Essbase Operations Each Hour



- Top 10 Longest Performing Essbase Data Extraction Operations

Top 10 Longest Performing Essbase Data Extraction Operations

Duration (Min:Sec)	Begin Time	End Time	Cube
19:47	13:22:02	13:41:48	FIN
04:44	14:08:12	14:12:56	FIN
01:01	14:05:09	14:06:10	FIN
01:01	14:02:39	14:03:40	FIN
01:00	13:46:49	13:47:49	FIN
00:58	14:15:09	14:16:07	FIN
00:54	04:19:42	04:20:36	FIN
00:53	14:06:50	14:07:44	FIN
00:36	00:58:36	00:59:13	FIN
00:34	13:43:07	13:43:41	FIN

Information in this table includes the start and end time, and cube from which data was extracted for each operation in the table. Depending on the total duration, you may need to evaluate and streamline these operations to improve performance.

- Top 10 Longest Performing Essbase Data Load Operations

Top 10 Longest Performing Essbase Data Load Operations

Duration (Min:Sec)	Begin Time	End Time	Cube
00:04	09:30:46	09:30:50	FIN
00:03	09:08:10	09:08:13	FIN
00:02	13:50:14	13:50:16	FIN
00:02	21:08:31	21:08:33	FIN
00:02	01:32:54	01:32:56	FIN
00:02	01:08:31	01:08:33	FIN
00:02	09:23:07	09:23:09	FIN
00:02	21:23:47	21:23:48	FIN
00:02	01:24:46	01:24:47	FIN
00:02	13:23:06	13:23:08	FIN

- Top 10 Longest Performing Block Storage (BSO) Restructure Operations
  This table lists the type of each restructure operation and the name of the cube that was restructured.

Top 10 Longest Performing *BSO Restructures*

Duration (Min:Sec)	Begin Time	End Time	Cube	Type
00:03	12:12:13	12:12:18	Plan1	Outline Only
00:02	12:18:32	12:18:34	Plan1	Full implicit (Refresh)
00:02	12:12:20	12:12:23	Plan3	Outline Only
00:02	12:15:29	12:15:32	Plan3	Outline Only
00:02	12:15:25	12:15:27	Plan1	Index Only Implicit (Refresh)
00:01	12:18:35	12:18:37	Plan2	Outline Only
00:01	12:12:18	12:12:20	Plan2	Outline Only
00:01	12:15:28	12:15:29	Plan2	Outline Only
00:01	12:21:36	12:21:38	Plan2	Outline Only
00:01	12:20:12	12:20:13	Plan1	Full Explicit/Forced

- Top 10 Longest Performing Essbase Queries Over 15 Seconds
  Top 10 Essbase queries that took over 15 seconds to execute.

Top 10 Longest Performing Essbase Queries over 15 seconds

Duration (Min:Sec)	Begin Time	End Time	Context	Query
02:08	03:21:44	03:23:52	DBNAME:RptFin .... See More	SELECT {[Period].[Sep],[Period].[Nov],[Period].[Jul],[Period].[Aug],[Period].[Oct],[Period].[Dec]} ON COLUMNS, ... See More
02:02	03:16:42	03:18:44	DBNAME:RptFin .... See More	,,,,,FY21,E1,T9,Activity_Rpt,,,,,,,,,, ... See More
01:56	03:51:18	03:53:14	DBNAME:RptFin .... See More	SELECT {[Period].[Dec]} ON COLUMNS,NON EMPTY {CROSSJOIN({[CostCode].[130010].Level.Members},CROSSJOIN(.... See More
01:50	03:48:35	03:50:25	DBNAME:RptFin .... See More	,,,,,FY21,E1,T9,Activity_Rpt,,,,,,,,,, ... See More
01:45	02:55:27	02:57:12	DBNAME:RptFin .... See More	SELECT {{CROSSJOIN({[FY21]},CROSSJOIN({[Actual]},CROSSJOIN({[Final]},CROSSJOIN({[YTD]},{[Mar]})))))}, ... See More
01:39	02:50:59	02:52:38	DBNAME:RptFin .... See More	SELECT {[Period].[Dec]} ON COLUMNS,NON EMPTY {CROSSJOIN({[Year].[FY20]},CROSSJOIN({[Scenario].[Rolling]}, ... See More
01:23	06:22:17	06:23:40	DBNAME:RptFin .... See More	SELECT {{CROSSJOIN({[FY21]},CROSSJOIN({[Actual]},CROSSJOIN({[Final]},CROSSJOIN({[YTD]},{[Mar]})))))}, ... See More
01:22	03:17:32	03:18:54	DBNAME:RptFin .... See More	SELECT {[Period].[Sep],[Period].[Nov],[Period].[Jul],[Period].[Aug],[Period].[Oct],[Period].[Dec]} ON COLUMNS, ... See More
01:20	03:26:40	03:28:00	DBNAME:RptFin .... See More	SELECT {[Period].[Oct]} ON COLUMNS,NON EMPTY {CROSSJOIN({[Year].[FY21]},CROSSJOIN({[Version].[Working]}, ... See More
01:02	23:01:24	23:02:26	DBNAME:ProfLoss .... See More	SELECT {{CROSSJOIN({[FY21]},CROSSJOIN({[Budget]},CROSSJOIN({[Working]},CROSSJOIN({[Month]},{[YearTotal]})))))}, ... See More

- Top 10 Essbase Queries by Total Duration
  Top 10 Essbase queries that were executed for the longest durations and the cube against which each query was run.

Top 10 Essbase Queries by Total Duration

Total Duration (Min:Sec)	Executions	Cube	Query
02:04	4	Consol	SELECT {CROSSJOIN({[FCCS_Periodic]},CROSSJOIN({[Entity Currency]},CROSSJOIN({[FCCS_Intercompany Top]}, ... See More
00:47	1	Consol	,,, ,Actual,Actual, ,FCCS_Total Cash,FCCS_Total Cash, ,[USA].[E1010],[USA].[E1010], ,FCCS_Periodic,FCCS_Periodic, ,Entity Currency,Entity Currency, ,FCCS_Intercompany Top,FCCS_Intercompany Top, ,FCCS_Data Input,FCCS_Data Input, ,FCCS_Local GAAP,FCCS_Loc...
00:32	1	Consol	,,,, ,FCCS_YTD,FCCS_YTD,FCCS_YTD, ,[Department].[Total Department],[Department].[Total Department],[Department].[Total Department], ,Total Location,Total Location,Total Location, ,Total Future Use,Total Future Use,Total Future Use, ,FCCS_Total Balance S...
00:27	1	Consol	,,,, ... See More
00:27	1	Consol	,,,, ... See More
00:27	1	Consol	SELECT {CROSSJOIN({[FCCS_Periodic]},CROSSJOIN({[Entity Currency]},CROSSJOIN({[FCCS_Intercompany Top]}, ... See More

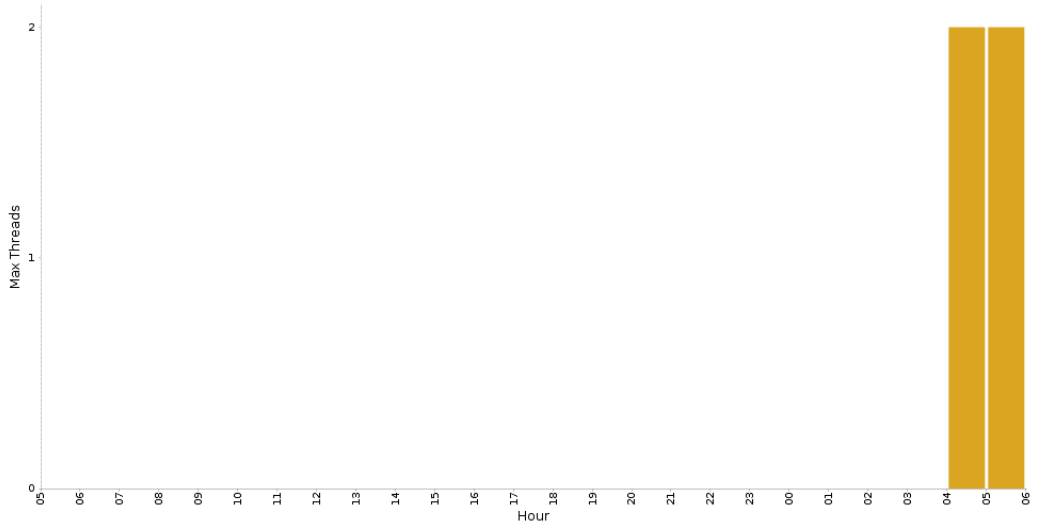
- Top 10 Essbase Queries by Execution
  Top 10 most frequently run Essbase queries and the cube against which each query was run.

Top 10 Essbase Queries by Execution

Executions	Total Duration (Min:Sec)	Cube	Query
4	02:04	Consol	SELECT {CROSSJOIN({[FCCS_Periodic]},CROSSJOIN({[Entity Currency]},CROSSJOIN({[FCCS_Intercompany Top]}, ... See More
1	00:27	Consol	,,,, ... See More
1	00:27	Consol	SELECT {CROSSJOIN({[FCCS_Periodic]},CROSSJOIN({[Entity Currency]},CROSSJOIN({[FCCS_Intercompany Top]}, ... See More
1	00:32	Consol	,,,, ,FCCS_YTD,FCCS_YTD,FCCS_YTD, ,[Department].[Total Department],[Department].[Total Department],[Department].[Total Department], ,Total Location,Total Location,Total Location, ,Total Future Use,Total Future Use,Total Future Use, ,FCCS_Total Balance S...

- Max Number of Calculation Threads
  This chart shows the maximum number of calculation threads during any given hour.

Max Number of Calculation Threads



Essbase Runtime Data

The Activity report may include the following Oracle Essbase runtime data:

Last 15 Data Management Clear Data Commands

This table logs recent Clear Data commands from Data Management, helping identify potential causes of data loss and verify alignment with intended activity. The table includes:

- Time - The timestamp indicating when the Clear Data command was executed.
- Process ID - The unique identifier assigned to the Data Management process that triggered the command.
- Command - The full Clear Data command issued.

Last 15 Calc Script Clear Data Commands

This table logs recent Clear Data commands executed through calculation scripts. It helps identify users responsible for the operation, the impacted cube, and the script details that triggered data clearance. The table includes:

- User – The user account that initiated the Clear Data operation.
- Cube – The name of the cube where the data was cleared.
- Calculation Script – The script used to execute the Clear Data command.
- Command – The specific command(s) within the script responsible for clearing the data.

Last 15 Calc Script Clear Block Commands

This table logs recent Clear Block commands issued via calculation scripts, helping audit user actions and block-level data changes.The table includes:

- **User** – The user account that ran the Clear Block operation.
- **Cube** – The name of the cube where blocks were cleared.
- **Calculation Script** – The script used to perform the Clear Block command.
- **Command** – The exact command(s) in the script that led to the block clearing.

Essbase Runtime Metrics

These metrics provide performance insights into recent Essbase operations over the past 24 hours.

Essbase Runtime Metric	Description
Essbase Requests Duration in Minutes	Total execution time of Essbase activities in the last 24 hours.
Average Essbase Calc Execution Duration in Seconds	Average time, in seconds, taken to run Essbase calculations in the last 24 hours.
Longest Essbase Calc Execution Duration in Seconds	Time, in seconds, taken by the longest running Essbase calculation in the last 24 hours.
Average Essbase Data Load Duration in Seconds	Average time, in seconds, taken by the Essbase data load activities in the last 24 hours.
Average Essbase Restructure Duration in Seconds	Average time, in seconds, taken by the Essbase restructure operations in the last 24 hours.

Essbase Runtime Metric	Description
Average Essbase Spread Sheet Extraction Duration in Seconds	Average time, in seconds, taken by the Essbase spread sheet extraction activities in the last 24 hours.
Longest Essbase Query Duration in Seconds	Time, in seconds, taken by the longest running Essbase query in the last 24 hours.
Average Essbase MDX Query Execution Duration in Seconds	Average time, in seconds, taken by the Essbase MDX query executions in the last 24 hours.

Essbase Design Metrics and Statistics

This section includes:

- Information related to the application such as the number of ASO and BSO cubes and their dimensions, and the highest number of total blocks in any Essbase cube.
- Statistics about each ASO and BSO cube in the application.

For more details, see Application Design and Runtime Information

Outline Warnings

The Outline Warnings table gives warnings for issues that would result in bad performance of forms and reports. The table has three columns:

- **Type** - Outline issue.
  Fixing these warnings helps avert potential calculation issues. Click a warning for more information and to review the troubleshooting tips available in the *Operations Guide*.
- **Cube** - Oracle Essbase cube whose members have the outline issue
- **Members** - List of members that have the outline issue

Outline Warnings

Type	Cube	Members
Dynamic Calc Level 0 Members Without A Formula	Vision.Plan1	[Account].[7006]
Dynamic Calc Level 0 Members Without A Formula	Vision.Plan2	[Scenario].[Plan Adj %], [Entity].[New York], [Entity].[Connecticut], [Entity].[Pennsylvania], [Entity].[Georgia], [Entity].[Nevada], ... See More
Dynamic Calc Level 0 Members Without A Formula	Vision.Plan3	[Scenario].[Plan Adj %], [Entity].[New York], [Entity].[Connecticut], [Entity].[Pennsylvania], [Entity].[Georgia], [Entity].[Nevada], ... See More
Dynamic Calc Members with Formula and Aggregating Children	Vision.Plan1	[Period].[YearTotal], [Period].[Q1], [Period].[Q2], [Period].[Q3], [Period].[Q4]
Generation 2 members that are not Never or Ignore but have Shared Member Descendants	BVision.Vis1ASO	[Entity].[Management Rollup]

Calculation Script Statistics

The Activity Reports contains the following information about calculation scripts that were executed in the environment:

- Top 5 longest running calculation scripts that took over one minute to execute.

Top 5 Longest Performing Calc Scripts Commands over 1 Min

Duration (Min:Sec)	Begin Time	End Time	Context	Calc Script Command
63:31	18:47:01	19:50:32	Cube name: ProfLoss .... See More	FIXPARALLEL (4, month, "FY21" : "FY26", "T9", "E1", @RELATIVE("FTOT", 0), "FTOT", "Rolling", "Working") .... See More
11:48	18:35:12	18:47:00	Cube name: ProfLoss .... See More	FIX ("FY21" : "FY26", @RELATIVE("FTOT", 0), "Rolling", Month, "E1", "T9", "0690_5", "0691_3", "0691_5", ... See More
11:22	18:08:30	18:19:52	Cube name: Employee .... See More	FIX (Jan : Dec, E1, Month, "Total_Jobs", "Rolling", "Working") .... See More
11:13	18:20:59	18:32:12	Cube name: ProfLoss .... See More	FIX (FY21) .... See More
10:33	13:38:49	13:49:22	Cube name: ProfLoss .... See More	FIXPARALLEL (4, Working) .... See More

- Top 10 Calc Script Commands By Number of Blocks Created

This table identifies the top 10 business rules that resulted in the creation of the largest number of blocks during the day.

Top 10 Calc Script Commands By Number of Blocks Created

Blocks Created	End Time	Cube	Calc Script	Calc Script Command
335,630	18:47:00	ProfLoss	ProfLoss_Night	FIX ("FY21" : "FY26", @RELATIVE("FTOT", 0), "Rolling", Month, "E1", "T9", "0690_5", "0691_3", "0691_5", ... See More
48	03:51:45	Employee	Employee Aggregate Data	FIX(Month,"Rolling","Working",FY21:FY24) .... See More
3	23:53:19	Employee	Employee Aggregate Data	FIX(Month,"Rolling","Working",FY21:FY24) .... See More

- Top 10 calculation scripts by average duration
  This table identifies the business rules that were executed for the longest duration. Available information includes the name of the calculation script, the number of times the script was run, and the average, minimum and maximum durations.

Top 10 Calc Scripts by Average Duration

Cube	Calc Script	Executions	Min Duration (Min:Sec)	Average Duration (Min:Sec)	Max Duration (Min:Sec)
FIN	FIN.BUD.COPYtoAVG.BAL.MEASURE.PY	1	09:39	09:39	09:39
FIN	FIN.PLN.AGG.FY20FY21.ScenarioSelect	3	04:15	04:32	05:02
FIN	FIN.ACT.AGG.Selected Periods	2	02:45	02:45	02:45
FIN	FIN.ACT.AGG.ACTUAL.Current_Month	4	02:19	02:32	02:53
FIN	FIN.ADMIN.SCENARIO.COPY	1	02:07	02:07	02:07
FIN	FIN.BUD.COPYtoAVG.BAL.MEASURE	1	01:51	01:51	01:51
FIN	FIN.ACT.COPYtoAVG.BAL.MEASURE_Current_Month	4	01:14	01:17	01:20
FIN	FIN.INPUT.COPYTOACTUALS	1	00:59	00:59	00:59
FIN	FIN.ACT.COPY.ACTUAL_SYSTEMtoACTUAL_Current_Month	4	00:18	00:19	00:23
Plan1	Calc Retail Client Portfolio	5	00:00	00:05	00:25

- Top 10 calculation scripts by execution.

Top 10 Calc Scripts by Executions

Executions	Calc Name
74	Weekly_Webform_Calculation
50	Load GL Actuals Current Year ? Closed Month
30	Fcst_Task
18	Fcst_GLMSBenefitsCalc
15	Weekly Task
9	Load GL Actuals Current Year
8	Fcst_OtherOperatedMain
4	Fcst_BanqCateringMainCalc
4	Fcst_OutRevOthExpCalc
3	Fcst_RoomsMainCalc

- Top 10 longest performing calculation scripts executions.

Top 10 Longest Performing Calc Scripts Executions				
Duration (Min:Sec)	Begin Time	End Time	Cube	Calc Script
09:39	12:21:27	12:31:06	FIN	FIN.BUD.COPYtoAVG.BAL.MEASURE.PY
05:02	13:50:07	13:55:09	FIN	FIN.PLN.AGG.FY20FY21.ScenarioSelect
04:18	12:38:31	12:42:49	FIN	FIN.PLN.AGG.FY20FY21.ScenarioSelect
04:15	14:09:50	14:14:05	FIN	FIN.PLN.AGG.FY20FY21.ScenarioSelect
02:53	09:32:27	09:35:20	FIN	FIN.ACT.AGG.ACTUAL.Current_Month
02:45	15:09:17	15:12:03	FIN	FIN.ACT.AGG.Selected Periods
02:45	15:28:41	15:31:27	FIN	FIN.ACT.AGG.Selected Periods
02:33	13:51:34	13:54:07	FIN	FIN.ACT.AGG.ACTUAL.Current_Month
02:22	21:32:53	21:35:15	FIN	FIN.ACT.AGG.ACTUAL.Current_Month
02:19	01:34:06	01:36:25	FIN	FIN.ACT.AGG.ACTUAL.Current_Month

Manual Database Access Information

Manual access to the relational database by running SQL commands is prohibited except under emergency situations, for example, when an environment becomes unresponsive. The general process for addressing such emergencies involves Oracle responding to a service request filed on behalf of the subscriber. The service request should give explicit permission to Oracle to manually access the relational database to address issues. Statistics on manual access of the database available in the **Manual SQL Executions** table of the Activity Report includes the following:

- **Time**: The time at which SQL commands were executed against the database
- **SR #**: The service request number based on which the database was manually accessed
- **SQL**: The SQL statements that were executed

This section of the report allows you to audit manual database activities. If you identify an unauthorized manual database access, add the information from this section to a service request so that Oracle can immediately investigate the incident and take remedial actions if needed.

Manual Essbase Access Information

Manual access to the Oracle Essbase database using MaxL commands is prohibited except under emergency situations in which Oracle needs such access to respond to a service request filed on behalf of the subscriber. The service request should give explicit permission to Oracle to manually access the Essbase database to address issues. Statistics on manual access of the database available in the **Manual MaxL Execution Count** table of the Activity Report includes the following:

- **Time**: The time at which the MaxL commands were executed against the database
- **SR #**: The service request number based on which the database was manually accessed
- **MaxL**: The MaxL command that was executed

You can use this table to audit manual Essbase access and the activities performed through such access. If you identify an unauthorized manual access, add the information from this section to a service request so that Oracle can immediately investigate the incident and take remedial actions, if needed.

Business Rules Information

The following information is available:

- Top 10 longest performing business rules that take more than 30 seconds to run.

Top 10 Longest Performing Business Rules over 30 Seconds

Duration (Min:Sec)	Begin Time	End Time	User	Cube	Business Rule	Run Time Prompt
95:17	18:20:59	19:56:16	Admin	ProfLoss	ProfLoss_Night	CostCode:"FTOT" .... See More
25:39	17:55:05	18:20:44	Admin	Employee	Employee_Night	PlanQUTCostCode:"FTOT" .... See More
10:33	13:38:49	13:49:22	Admin	ProfLoss	ProfLoss_Copy_Rolling_to_Backup	
04:53	22:50:05	22:54:58	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Rolling" .... See More
04:18	13:49:22	13:53:40	Admin	Employee	Employee_Copy_Rolling_to_Backup	
03:58	08:00:06	08:04:04	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Budget" .... See More
03:32	05:50:05	05:53:37	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Rolling" .... See More
03:25	06:50:06	06:53:31	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Rolling" .... See More
03:12	23:50:06	23:53:19	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Rolling" .... See More
02:59	04:50:06	04:53:05	Admin	Employee	Employee Aggregate Data	Emp_Scenario:"Rolling" .... See More

- Top 10 Business Rules by Execution
  This table enables you to monitor the performance of business rules in the application.

Top 10 Business Rules by Execution

Executions	Business Rule	Average Duration (Min:Sec)	Unique Users
1	ProfLoss_Night	95:17	1
1	Employee_Night	25:39	1
1	ProfLoss_Copy_Rolling_to_Backup	10:33	1
10	Employee Aggregate Data	03:12	1
1	Employee_Copy_Rolling_to_Backup	04:18	1
23	PL - Calculate GL for Desc of Selected CostCode	00:34	4
1	CalcP799YTD	01:31	1
28	PL CostCode RollUp	00:15	10
1	CalcHier	00:34	1
1	Employee_Update_ProfLoss_Sessionals_Form	00:28	1
1	PL - CostCode RollUp_Sessional_Form2	00:22	1

- Business rules that take more than 3 seconds to run.

Business Rules Attached to a Form Taking Longer than 3 Seconds

Duration (Min:Sec)	Time (PST)	User	Form	Business Rule	Run Time Prompts
00:03	07:18:38	jdoe	Other Operated PL - Forecast	Fcst_OtherOperatedMain	rtp_Department:"D11202" .... See More
00:03	13:07:47	janedoe	Rooms PL - Forecast	Fcst_RoomsMainCalc	rtp_Department:"D11010" .... See More

Application Design and Runtime Information

This section gives a list of application design and runtime metrics labels with their descriptions.

Table 12-3 Essbase Design Metrics

Design Metric	Description
Oracle Essbase ASO Cubes	Number of ASO cubes in Essbase.
Max Essbase ASO Dimensions	Number of dimensions in the ASO cube that has the highest number of dimensions.
Max Essbase ASO Total Size in MB	Size, in MB, of the largest ASO database.
Essbase BSO Cubes	Number of BSO cubes in Essbase
Max Essbase BSO Standard Dimensions	Largest number of standard dimensions, other than Attribute dimension, in any of the BSO cubes
Max Essbase BSO Sparse Dimensions	Number of sparse dimensions, other than attribute dimension, in BSO cube with the highest number of sparse dimensions.
Max Essbase BSO Dense Dimensions	Number of dense dimensions in the BSO cube with the highest number of dense dimensions.
Max Essbase BSO Attribute Dimensions	Number of attribute dimensions in the BSO cube with the highest number of attribute dimensions.
Max Essbase Total Blocks	Number of blocks in the BSO cube with the highest number of blocks.
Max Essbase Block Size in KB	Size, in KB, of the block with the largest size in any of the BSO cubes.
Max Essbase Cells in Millions	Number of cells, in millions, in the BSO cube with the highest number of cells.
Max Essbase Level 0 Blocks	Number of level 0 blocks in the BSO cube with the highest number of level 0 blocks.
Max Essbase Upper Level Blocks	Number of upper level blocks in the BSO cube with the highest number of upper level (non-level 0) blocks.
Max Essbase Upper Level Blocks Percentage	Percentage of upper level blocks, with respect to the total number of blocks, in the BSO cube with the highest percentage of upper level blocks.
Max Essbase Page File Size in MB	Page file size, in MB, in the BSO cube with the largest Essbase page file.
Max Essbase Index File Size in MB	Index file size, in MB, in the BSO cube with the largest Essbase index file.
Max Essbase BSO Outline File Size in MB	BSO cube outline file size in MB. Large file size, usually, results if you use many dimensions with a large number of members.

Table 12-3 (Cont.) Essbase Design Metrics

Design Metric	Description
Max Essbase Hourglass/Modified Hourglass Deviations on Dense	Number of deviations in the current model from the hourglass or modified hourglass model for dense dimensions in the BSO cube with the largest number of deviations. In the hourglass model, dimensions in a BSO cube are ordered from the largest dense dimension to the smallest dense dimension followed by the smallest sparse dimension to the largest sparse dimension. In the modified hourglass model, dimensions in a BSO cube are ordered from the largest dense dimension to the smallest dense dimension, then by the smallest aggregating sparse dimension to the largest aggregating sparse dimension, and then by the non-aggregating sparse dimensions.
Max Essbase Hourglass Deviations on Sparse	Number of deviations in the current model from the hourglass model for sparse dimensions in the BSO cube with the largest number of deviations.
Max Essbase Modified Hourglass Deviations on Aggregating Sparse	Number of deviations in the current model from the modified hourglass model for aggregating sparse dimensions in the BSO cube with the largest number of deviations.
Min Essbase Clustering Ratio Percentage	Essbase clustering ratio of the BSO cube with the lowest Essbase clustering ratio. Essbase clustering ratio is a measure of fragmentation of page files. The maximum clustering ratio is 1, which indicates no fragmentation. The lower the clustering ratio, the more fragmented the Essbase database.
Hybrid enabled	Identifies whether the Essbase version on the current environment supports hybrid cubes. For detailed information, see About Essbase in Cloud EPM.

Application size

This section of the report explores the size of the application. Information available includes the data size (includes the size of snapshots and files available in the inbox and outbox), size of Essbase data, and the size of the maintenance snapshot.

Essbase BSO and ASO Cube Statistics

These sections provide statistics about each ASO and BSO cube in the application.

- Statistics available for every BSO cube:
  - Number of Total, Standard, Dense, Sparse, and Attribute Dimensions
  - Block Size in Cells and KB
  - Number of Total, Level 0, and Upper Level Blocks
  - Percentage of Upper Level Blocks
  - Number of Essbase Cells in Million
  - Essbase Density- Block Density and Average Clustering Ratio
  - Page File and Index File Sizes in MB

  - Data Cache and Index Cache Settings in MB
  - Essbase BSO Outline File Size in MB
  - Number of Deviations from the Hourglass/Modified Hourglass Model for Dense Dimensions
  - Number of Deviations from the Hourglass Model for Sparse Dimensions
  - Number of Deviations from the Modified Hourglass Model for Aggregating Sparse Dimensions
  - Number of Data Load, Restructure, Calc Execution, and Spreadsheet Extraction operations
- Statistics available for every ASO cube:
  - Number of Total and Attribute Dimension
    For Attribute dimension, shows Type and Base dimension
  - Maximum Key Length in Bits and Bytes
  - Number of Input-level Cells, Incremental Data Slices, Incremental Input Cells, Aggregate Views, Aggregate Cells, and Incremental Aggregate Cells
  - Percentage Time of Querying Incremental Data Slices
  - Total, Input-level Data, and Aggregate Data Sizes in MB
  - Pending Cache Size Limit in MB
  - Number of Restructure and Spreadsheet Extraction operations

Dimensions for Cube

Shows **statistics** and **dimension order** for each cube within the application, assisting in reviewing the usage order and performance metrics. The list is organized according to the dimension order in the application, which affects how Essbase calculates the dimensions. it also shows the member type or property (dense or sparse). For attribute dimensions, this table shows the attribute dimension type and the base dimension. Additionally, the table includes the total number of dimension members based on various settings such as data storage type (Store, Never Share, Label Only, Shared Members, Dynamic Calc and Store, and Dynamic Calc) and the operators being used.

You can also take valuable insights into Runtime Stored Levels and Bits Used, enabling more effective diagnosis of ASO Rule Performance issues.

Dimensions for Consol (BSO)

Outline Order	Name	Type/ Properties	Declared Members	Stored Members	Levels	Formulas	Store	Never Share	Label Only	Shared Members	Dynamic Calc and Store	Dynamic Calc	Add Operator	Sub Operator
1	Period	Dense	19	14	4	5	13	1				5	1	
2	Movement	Dense	157	116	8	11	1	115		5		36	143	6
3	Consolidation	Sparse	17	11	7	1	10	1	1			5	10	
4	Data Source	Sparse	1,032	1,026	5		12	1,014	2			4	16	
5	Currency	Sparse	91	89	3		6	83	2				1	
6	Account	Sparse	2,843	1,532	17	26	1,075	457	8	609		694	2,396	15
7	Intercompany	Sparse	760	757	4			757				3	759	
8	MRU	Sparse	694	501	13		1	500		1		192	692	
9	Analysis	Sparse	55	40	4	5	1	39		1		14	47	
10	Custom 3	Sparse	4	2	3		1	1		1		1	2	
11	Custom 4	Sparse	4	2	3		1	1		1		1	2	
12	Scenario	Sparse	3	3	2			3					1	
13	Years	Sparse	7	7	2		6	1					1	
14	View	Sparse	8	3	3	4		3	1			4	1	
15	Entity	Sparse	1,822	1,822	13		1	1,821					1	
16	Country	Attr_Text (Entity)	93	0	2							93	1	

Account Reconciliation Metrics

- Account Reconciliation Execution Statistics
- Account Reconciliation Configuration Metrics
- Account Reconciliation Runtime Metrics

Account Reconciliation Execution Statistics

This section includes:

- Top 10 Reports by Execution
- Top 10 Reports by Duration over 30 Seconds
- Top 10 Data Load Jobs by Duration over 30 Seconds
- Top 10 Other Jobs by Duration over 30 Seconds
- Top 10 Job Types by Execution

Top 10 Reports by Execution

This table lists 10 most frequently generated Account Reconciliation reports, how many times in the last 24 hours they were generated and by how many unique users, and the average time taken to generate each of them.

Top 10 Reports by Execution

Executions	Unique Users	Report Name	Average Duration(Min:Sec)
2	1	Dataload Staging Table Report	02:21
2	2	BSSC Account Detail Report	00:56
1	1	Audit Prepaid Expenses and Other Current Assets	02:42

Top 10 Reports by Duration over 30 Seconds

This table lists top 10 Account Reconciliation reports that took more than 30 seconds to be generated. This table identifies the time taken to generate the report, the user who initiated the report generation, start and end times, name of the report, and the report context including format, parameters, size of the generated report, number of rows and columns and the SQL query that was used to gather the data for the report.

Top 10 Reports by Duration over 30 Seconds

Duration (Min:Sec)	User	Begin Time	End Time	Report Name	Context
03:22	xxxxxxx@example.com	09:01:06	09:04:28	Dataload Staging Table Report	Format: CSV ... See More
02:42	xxxxxxx@example.com	14:22:37	14:25:20	Audit Prepaid Expenses	Format: XLSX ... See More
01:21	xxxxxxx@example.com	09:07:42	09:09:04	Dataload Staging Table Report	Format: CSV ... See More
01:04	xxxxxxx@example.com	14:47:52	14:48:57	BSSC Account Detail Report	Format: XLSX ... See More

Top 10 Data Load Jobs by Duration over 30 Seconds

This table lists the top 10 data load jobs that took more than 30 seconds to complete. This table identifies the time taken to complete the job, the user who initiated it, job start and end times, job name, and job context including Period for which the data load was performed, status of the job, and the number of errors and warning reported for the job.

Top 10 Data Load Jobs by Duration over 30 Seconds

Duration (Min:Sec)	User	Begin Time	End Time	Job Name	Context
09:13	xxxxxxx@example.com	07:57:17	08:06:31	GL Functional_Recalculate	Period Name: Aug 2021 Status: STAGING_COMPLETED Error Count: 0 Warning Count: 1
01:02	xxxxxxx@example.com	08:24:35	08:25:37	GL_Entered_Recalculate	Period Name: Aug 2021 Status: STAGING_COMPLETED Error Count: 0 Warning Count: 1
00:58	xxxxxxx@example.com	08:06:32	08:07:31	GL Functional_Recalculate	Period Name: Aug 2021 .... See More
00:34	xxxxxxx@example.com	08:07:32	08:08:06	GL Functional_Recalculate	Period Name: Aug 2021 .... See More

Top 10 Other Jobs by Duration over 30 Seconds

This table lists the top 10 jobs other than data load jobs that took more than 30 seconds to complete. This table identifies the time taken to complete the job, the user who initiated it, job start and end times, job name, and job context, if any. User name is not displayed for maintenance jobs that Oracle Fusion Cloud Enterprise Performance Management runs.

Top 10 Other Jobs by Duration over 30 Seconds

Duration (Min:Sec)	User	Begin Time	End Time	Job Name	Context
00:37	epmuser	06:45:00	06:45:37	System Maintenance	Job Type: SYNC _USERS

Top 10 Job Types by Execution

This table lists the top 10 jobs by job types. For every job type, it shows the number of times the job was run and the average duration of each run.

Top 10 Job Types by Execution

Executions	Job Type	Average Duration (Min:Sec)
48	DATA LOAD	13:33
47	EMAIL NOTIFICATIONS	07:08
37	IMPORT TRANS	01:33
5	GENERATE REPORT	09:53
4	DELETE RECONCILIATIONS	00:03
4	EXPORT QUERY AS CSV UNMATCH	00:01
3	DELETE PROFILES	01:27
3	IMPORT	00:07
2	COPY TO PERIOD	14:42
1	AUTO MATCH	28:36

Account Reconciliation Configuration Metrics

This section includes:

- Account Reconciliation Configuration Metrics
- Account Reconciliation Transaction Matching Configuration Metrics

Account Reconciliation Configuration Metrics

Label in Activity Report	Description
ARCS Profiles	Total number of profiles
ARCS Attributes	Total number of custom attributes
ARCS Calculated Attributes	Total number of calculated custom attributes
ARCS Custom Reports	Total number of custom reports
ARCS Maximum Attributes per Profile	Largest number of custom attributes associated with one profile
ARCS Maximum Questions per Profile	Largest number of questions on one profile
ARCS Total Frequencies	Total number of frequencies
ARCS Periods	Total number of periods
ARCS Average Periods per Calendar Year	Average number of periods whose start date is in a calendar year. 0 if there are no calendar years
ARCS Org Units	Total number of organizational units
ARCS Average Attributes per Profile	Average number of custom attributes associated with a profile
ARCS Average Questions per Profile	Average number of questions on a profile

Account Reconciliation Transaction Matching Configuration Metrics

Label in Activity Report	Description
ARCS TM Total Profiles	Total number of profiles associated with Transaction Matching

Label in Activity Report	Description
ARCS TM Maximum Profiles per Match Type	Number of profiles in the match type with the largest number of profiles
ARCS TM Average Profiles per Match Type	Average number of profiles in a match type
ARCS TM Maximum Transaction Attributes per Profile	Number of transaction attributes in the profile containing the largest number of transaction attributes
ARCS TM Match Types	Total number of match types
ARCS TM Match Processes	Total number of match processes
ARCS TM Data Sources	Total number of Transaction Management data sources
ARCS TM Maximum Rules per Match Processes	Number of rules in the match process with the largest number of rules
ARCS TM Maximum Attributes per Data Source	Number of attributes in data source with the largest number of attributes
ARCS TM Maximum Data Sources per Match Type	Number of data sources in the match type with the largest number of data sources

Account Reconciliation Runtime Metrics

This section includes:

- Account Reconciliation-Related Runtime Metrics
- Account Reconciliation Transaction Matching Runtime Metrics

Account Reconciliation-Related Runtime Metrics

Label in Activity Report	Description
ARCS Total Reconciliations	Total number of Account Reconciliations
ARCS Open Reconciliations	Total number of Account Reconciliations in Open status
ARCS Latest Open Period: Text	Name of the latest period by end date in Open status
ARCS New Reconciliation Transactions in 1 Day	The number of new Account Reconciliation transactions created in the last day
ARCS Closed Reconciliations in 1 Day	Total number of Account Reconciliations closed since yesterday
ARCS Closed Reconciliations in last 30 Days	Total number of Account Reconciliations closed in the last 30 days
ARCS Auto Closed Reconciliations in 1 Day	The number of Account Reconciliations that were auto-closed or both auto-submitted and auto-approved in the last 24 hours
ARCS Auto Closed Reconciliations in last 30 Days	The number of Account Reconciliations that were auto-closed or both auto-submitted and auto-approved in the last 30 days
ARCS Active Periods	The number of periods that are in Open or Closed status
ARCS Active Reconciliations	The number of Account Reconciliations in Open status in active periods
ARCS Active Summary Reconciliations	The number of Summary Account Reconciliations in Open status in an active period

Label in Activity Report	Description
ARCS Maximum Transactions per Open Reconciliation	Largest number of transactions associated with an open Account Reconciliation in an open period
ARCS Maximum Reconciliation Transactions for Open Periods	Average number of Account Reconciliation transactions associated with an open reconciliation in an open period
ARCS Average Reconciliation Transactions for Open Periods	Average number of Account Reconciliation transactions in an open period
ARCS Standard Deviation of Reconciliation Transaction for Open Periods	Standard deviation of Account Reconciliation transactions in an open period
ARCS Total Attachments	The number of attachments in open periods
ARCS Size of Attachments in MB	Size, in MB, of attachments in open periods
ARCS Percentage of Auto Closed Reconciliations in Last 30 Days	Percentage of Account Reconciliations that were either auto-closed or auto-submitted and auto-approved in the last 30 days
ARCS Auto Closed Balance Sheet Reconciliations in Last 30 Days	The number of Account Reconciliations with the Balance Sheet process that were either auto-closed or auto-submitted and auto-approved in the last 30 days
ARCS Percentage of Auto Closed Balance Sheet Reconciliations in Last 30 Days	Percentage of Account Reconciliations with the Balance Sheet process that were either auto-closed or auto-submitted and auto-approved in the last 30 days
ARCS Percentage of Rejected Reconciliations in Last 30 Days	Percentage of manually closed Account Reconciliations in the last 30 days that had at least one rejection * (see Note)
ARCS Percentage of Rejected Balance Sheet Reconciliations in Last 30 Days	Percentage of manually closed Account Reconciliations in the last 30 day with the Balance Sheet Process that had at least one rejections* (see Note)
ARCS Percentage of Late Reconciliations in Last 30 Days	Percentage of manually closed Account Reconciliations in the last 30 days that were ever late for anyone in the workflow * (see Note)
ARCS Percentage of Late Balance Sheet Reconciliations in Last 30 Days	Percentage of manually closed Account Reconciliations in the last 30 days with the Balance Sheet process that were ever late for anyone in the workflow * (see Note)
ARCS Average Reconciliation Duration in Last 30 Days	Average duration (in days), from the Open date to the Close date, of Account Reconciliations that were manually closed in the last 30 days * (see Note)
ARCS Average Balance Sheet Reconciliation Duration in Last 30 Days	Average duration in days, from the Open date to the Close date, of Account Reconciliations with the Balance Sheet process that were manually closed in the last 30 days * (see Note)
ARCS Average Reconciliation Preparation Duration in Last 30 Days	Average duration (in days), from the Open date to the latest submission date, of Account Reconciliations that were manually closed in the last 30 days * (see Note)
ARCS Average Balance Sheet Reconciliation Preparation Duration in Last 30 Days	Average duration (in days), from the Open date to the latest submission date, of Account Reconciliations with the Balance Sheet process that were manually closed in the last 30 days * (see Note)

Label in Activity Report	Description
ARCS Average Reconciliation Review Duration in Last 30 Days	Average duration (in days)s, from the latest preparer submission date to the closed date, of Account Reconciliations that have at least one reviewer and were manually closed in the last 30 days * (see Note)
ARCS Average Balance Sheet Reconciliation Review Duration in Last 30 Days	Average duration (in days), from the latest submission date to the closed date, of Account Reconciliations with the Balance Sheet process that have at least one reviewer and were manually closed in the last 30 days * (see Note)
ARCS Average Completed Reconciliation per Preparer in Last 30 Days	Average number of Account Reconciliations manually submitted by each preparer that were closed in the last 30 days * (see Note)
ARCS Average Completed Balance Sheet Reconciliation per Preparer in Last 30 Days	Average number of Account Reconciliations with the Balance Sheet process manually submitted by each preparer that were closed the last 30 days * (see Note)
ARCS Average Completed Reconciliation per Reviewer in Last 30 Days	Average number of manually closed Account Reconciliations that each unique reviewer handled in the last 30 days * (see Note)
ARCS Average Completed Balance Sheet Reconciliation per Reviewer in Last 30 Days	Average number of manually closed Account Reconciliations with the Balance Sheet process that each unique reviewer handled in the last 30 days * (see Note)
ARCS Average Number of Reviewers per Reconciliation in Last 30 Days	Average number of reviewer levels on manually closed Account Reconciliations in the last 30 days
ARCS Average Number of Reviewers per Balance Sheet Reconciliation in Last 30 Days	Average number of reviewer levels on manually closed Account Reconciliations with the Balance Sheet process in the last 30 days
ARCS Formats Used on Closed Reconciliations in Last 30 days	The number of different formats used on Account Reconciliations closed in the last 30 days
ARCS Formats Used on Closed Transaction Matching Reconciliations in Last 30 days	The number of different formats used on Account Reconciliations associated with Transaction Matching and closed in the last 30 days
ARCS Formats Used on Closed Variance Analysis Reconciliations in Last 30 days	The number of different formats used on Account Reconciliations associated with Variance Analysis that were closed in the last 30 days
ARCS Pending Jobs in 1 day	Total number of Account Reconciliation jobs that entered a pending state within the past 24 hours
ARCS Pending Jobs in 30 days	Total number of Account Reconciliation jobs that entered a pending state over the past 30 days
Notes: * 0 if no manually closed records in the last 30 days	

Account Reconciliation Transaction Matching Runtime Metrics

Label in Activity Report	Description
ARCS TM Total Matches in 1 Day	Total number of matches created in the last 24 hours

Label in Activity Report	Description
ARCS TM Total Matches in Last 30 Days	Total number of matches created in the last 30 Days
ARCS TM Suggested Matches in 1 Day	Total number of suggested matches in the last 24 hours
ARCS TM Suggested Matches in Last 30 Days	Total number of suggested matches in the last 30 days
ARCS TM Manual Matches in 1 Day	Total number of manual matches created in the last 24 hours
ARCS TM Manual Matches in Last 30 Days	Total number of manual matches created in the last 30 days
ARCS TM Transactions Matched in 1 Day	Total number of transactions auto-matched in the last 24 hours
ARCS TM Transactions Matched in Last 30 Days	Total number of transactions auto-matched in the last 30 days
ARCS TM Maximum Transactions per Data Source	Maximum number of transactions in any data source
ARCS TM Total Transactions	Total transactions loaded into Transaction Matching till date
ARCS TM Transactions Loaded in 1 Day	Total transactions loaded in last 24 hours
ARCS TM Transactions Loaded in Last 30 Days	Total transactions loaded in last 30 days
ARCS TM Import Jobs in 1 Day	Total Import transactions jobs executed in last 24 hours
ARCS TM Import Jobs in 30 Days	Total Import transactions jobs executed in last 30 days
ARCS TM Automatch Jobs in 1 Day	Total auto-match jobs executed in last 24 hours
ARCS TM Automatch Jobs in 30 Days	Total auto-match jobs executed in last 30 days
ARCS TM Transactions Supported in 1 Day	Total number of transactions supported in the last 24 hours
ARCS TM Transactions Supported in Last 30 Days	Total number of transactions supported in the last 30 days

Enterprise Journal Runtime Metrics

The Activity report presents the following Enterprise Journal Runtime Metrics:

Label in Activity Report	Description
EJ Journal Periods	Total number of Journal Periods
EJ Used Journal Periods	Total number of Journal Periods that have been used (status - not pending)
EJ Active Journal Periods	Total number of Active Journal Periods (Open or Closed)
EJ Latest Open Journal Period	Name of the Latest Open Journal Period
EJ Templates Deployed	Total number of times Templates were deployed in Journal Periods. For example, if one Template was deployed in four Journal Periods, the value would be 4

Label in Activity Report	Description
EJ Templates Deployed in active Journal Periods	Total number of times Templates were deployed in Active Journal Periods. For example, if one Template was deployed into four Journal Periods, but only two were currently Active, the value would be 2
EJ Journals	Total number of Journals
EJ Open Journals	Total number of Journals in an Open status
EJ Posted Journals	Total number of Journals set to Posted status
EJ Ad-Hoc Journals	Total number of Ad-Hoc Journals of any status
EJ Recurring Journals	Total number of Recurring Journals of any status
EJ Posted Journals to Cloud Financials Target	Total number of Journals posted to Cloud Financials by direct integration
EJ New Journals in 1 day	Number of new Journals created in the last day by either Ad-Hoc or Recurring deployment. If Journals were re-deployed over existing Journals, they will only be counted as new if the original journals were deleted
EJ Opened Journals in 1 day	Number of Journals set to an Open status in the last day. This includes Journals that were reopened
EJ Closed Journals in 1 day	Number of Journals set to a Closed workflow status in the last day
EJ Posted Journals in 1 day	Number of Journals set to a Posted status in the last day
EJ New Journals in Last 30 days	Number of new Journals created in the last 30 days by either Ad-Hoc or Recurring deployment. If Journals were re-deployed over existing Journals, they will be counted as new only if the original journals were deleted.
EJ Opened Journals in Last 30 days	Number of Journals set to an Open status in the last 30 days. This includes Journals that were reopened
EJ Closed Journals in Last 30 days	Number of Journals set to a Closed workflow status in the last 30 days
EJ Closed Late Journals in Last 30 days	Number of Journals set to a Closed workflow status in the last 30 days that had ever been late
EJ Average Duration of Closed Journals in Last 30 days	Average duration (in days) for Journals set in Closed status in the last 30 days. Duration is calculated from the time the Journal was open to the time it was closed
EJ Posted Journals in Last 30 days	Number of Journals that were set to a Posted status in the last 30 days
EJ Average Duration of Posted Journals in Last 30 days	Average duration (in days) for Journals set to a Posted status in the last 30 days. Duration is calculated from the time the Journal was Ready To Post to the time it was set to Posted
EJ Posted Journals to Cloud Financials Target in 1 day	Number of Journals posted to Cloud Financials by direct integration in the last day
EJ Posted Journals to Cloud Financials Target in Last 30 Days	Number of Journals posted to Cloud Financials by direct integration in the last 30 days
EJ References	Total number of files uploaded
EJ References By Used Size in MB	Total size in MB of all files uploaded
EJ Alerts on Journals in Last 30 days	Number of Alerts associated with Journals in the last 30 days
EJ Closed Alerts on Journals in Last 30 Days	Number of Alerts associated with Journals set to the closed Status in the last 30 days

Profitability and Cost Management Design and Runtime Metrics

Profitability and Cost Management Design Metrics

This section provides design information such as the number of POV and models, and the maximum number of rules in a model. It also contains similar information for archived models.

Profitability and Cost Management Design Metrics

Metric Name	Value
PCM POVs	12
PCM Models	1
PCM Maximum Number of Rules in a Model	21
PCM Archived Models	1
PCM Rules across all Archived Models	21
PCM Maximum Number of Rules in an Archived Model	21

Profitability and Cost Management Runtime Metrics

This section provides run time information such as the number of calculations run in one day and number of calculations run in the last 30 days.

Profitability and Cost Management Runtime Metrics

Metric Name	Value
PCM Statistics	24,768
PCM Total Calculation Executions in Lifetime	12
PCM Statistics Gathered in the Last 30 Days	24,768
PCM Total Calculation Executions in the Last 30 Days	12
PCM Calculation Runs in 1 Day	12
PCM Longest Calculation Duration in Minutes in Lifetime	4.87
PCM Longest Calculation Duration in Minutes in the Last 30 Days	4.87
PCM Average Calculation Duration in Minutes in the Last 30 Days	4.44
PCM Longest Single Custom Calc Rule Duration in Minutes in the Last 30 Days	0
PCM Longest Single Allocation Rule Duration in Minutes in the Last 30 Days	0.58
PCM Largest Count of Rules Executed in a Job in the Last 30 days	93
PCM Average Count of Rules Executed in a Job in the last 30 days	84
PCM Largest Updated Cell Count of Rules Executed in the Last 30 Days	912,832
PCM Average Updated Cell Count of Rules Executed in the Last 30 days	33,354

Supplemental Data Manager Design and Runtime Metrics

This section gives a list of Supplemental Data Manager design and runtime metrics labels with their descriptions.

Table 12-4 Supplemental Data Manager Design Metrics

Metrics Label	Description
SDM Local Dimensions	Total number of local dimensions. This does not include default system dimensions.
SDM Collection Intervals	Total number of collection intervals.
SDM Maximum Collections per Collection Interval	Maximum number of collections associated with a single collection interval.
SDM Total Collections	Total number of collections.
SDM Total Sub Collections	Total number of sub collections.
SDM Max Sub Collection per Collection	Maximum number of sub-collections associated with a single collection.
SDM Attributes	Total number of attributes.
SDM Attributes - Calculated	Total number of calculated attributes.
SDM Maximum Attributes per Collection/ Sub Collections	Maximum number of attributes associated with a single collection or sub-collection.
SDM Form Templates	Total number of form templates.
SDM Maximum Sections on Form Template	Maximum number of sections on a single template.
SDM Average Sections on Form Template	Average number of sections on form templates.
SDM Form Templates Workflow - Post only	Number of form templates with post only workflow.
SDM Maximum Form Template Workflows	Maximum number of workflows on a single template.
SDM Average Form Template Workflows	Average number of workflows on form template.
SDM Maximum Questions per Form Template	Maximum number of questions on a single form template.

Table 12-5 Supplemental Data Manager Runtime Metrics

Metrics Label	Description
SDM Data Collection Periods	Total number of data collection periods.
SDM Used Data Collection Periods	Total number of data collection periods that have been used (not pending).
SDM Active Data Collection Periods	Total number of active (open or closed) data collection periods.
SDM Templates Deployed	Total number of times that the templates are deployed in all data collection periods. For example, if one template was deployed four different times, the result would be 4.
SDM Templates Deployed in Active Data Collection Periods	Total number of times the templates are deployed in active (open or closed) data collection periods. For example, if one template was deployed into four data collection periods, but only two were currently active, the result would be 2.
SDM Forms	Total number of forms.
SDM Open Forms	Total number of forms in an open status.
SDM Ad-Hoc Forms	Total number of ad-hoc forms in any status.
SDM Forms in Active Collection Periods	Total number of forms in active (open or closed) collection periods.

Table 12-5 (Cont.) Supplemental Data Manager Runtime Metrics

Metrics Label	Description
SDM Open Forms in Active Collection Periods	Total number of forms in active collection periods with open status.
SDM Closed Forms in Active Data Collection Periods	Total number of forms in active collection periods with closed status.
SDM New Forms (1 day)	Number of new forms created in the last day by either ad-hoc or recurring deployment.
SDM Redeployed Forms (1 day)	Number of existing recurring forms that were redeployed in the last day.
SDM Opened Forms (1 day)	Number of forms that were set to an open status in the last day. This includes forms that were reopened.
SDM Closed Forms (1 day)	Number of forms that were set to a closed workflow status in the last day.
SDM Closed Late Forms (30 days)	Number of forms that were set to a closed workflow status in the last 30 days that had ever been late.
SDM Rejected Forms (30 days)	Number of forms that were rejected in the last 30 days. If the same form was rejected multiple times, it still counts as one.
SDM Average Duration of Closed Forms (30 days)	Average duration of forms that have been set to a closed workflow status. Duration is calculated from the time the form was open to the time it was closed, which includes posting time if applicable.
SDM New Forms (30 days)	Number of new forms created in the last 30 days by either ad-hoc or recurring deployment.
SDM Redeployed Forms (30 days)	Number of existing recurring forms that were redeployed in the last 30 days.
SDM Opened Forms (30 days)	Number of forms that were set to an open status in the last 30 days. This includes forms that were reopened.
SDM Closed Forms (30 days)	Number of forms that were set to a closed workflow status in the last 30 days.
SDM References	Total number of files uploaded.
SDM References By Size (Used) in MB	Total size in MB of all files uploaded.
SDM Form Alerts (30 days)	Number of alerts associated with forms in the last 30 days.
SDM Closed Form Alerts (30 Days)	Number of alerts associated with forms set to closed status in the last 30 days.

Task Manager Design and Runtime Metrics

This section gives a list of Task Manager design and runtime metrics labels with their descriptions.

Table 12-6 Task Manager Design Metrics

Metrics Label	Description
Task Manager Org Units	Total number of organizational units
Task Manager Custom Attributes	Total number of custom attributes
Task Manager Calculated Attributes	Total number of calculated custom attributes
Task Manager Alert Types	Total number of alert types
Task Manager Custom Integrations	Total number of custom integrations
Task Manager Task Types	Total number of task types
Task Manager Custom Task Types	Total number of custom task types
Task Manager Task Types with URL Integration	Total number of task types associated with an end user integration and used in a template or active schedule task
Task Manager Task Types with Automation Integration	Total number of task types that have an automation integration and used in a template or active schedule task
Task Manager Task Types with Event Monitor Integration	Total number of task types that have an event monitoring integration and used in a template or active schedule task
Task Manager Manual Task Types	Total number of custom task types that are not based on an integration
Task Manager Templates	Total number of templates
Task Manager Maximum Embedded Templates	Maximum number of embedded templates on a single parent template
Task Manager Average Embedded Templates	Average number of embedded templates on a single parent template * (see Note) Does not include non-parent templates.
Task Manager Template Tasks	Total number of tasks on all templates
Task Manager Template Tasks with URL Integration	Total number of tasks on all templates from a custom task type associated with an end user integration
Task Manager Template Tasks with Automation Integration	Total number of tasks on all templates from a custom task type associated with an automated integration
Task Manager Template Task with Event Monitor Integration	Total number of tasks on all templates from a custom task type associated with an event monitoring integration
Task Manager Basic Template Tasks	Total number of tasks on all basic type templates
Task Manager Parent Template Tasks	Total number of tasks on all parent type templates
Task Manager Manual Template Tasks	Total number of tasks on all templates from custom task types that are not associated with an integration
Task Manager Average Tasks per Template	Average number of tasks per template * (see Note)
Task Manager Maximum Attributes per Template Task	Maximum number of custom attributes on a template task
Task Manager Average Attributes per Template Task	Average number of custom attributes on each template task * (see Note)
Task Manager Maximum Questions per Template Task	Maximum number of questions on each template task
Task Manager Average Questions per Template Task	Average number of questions on each template task * (see Note)

Table 12-6 (Cont.) Task Manager Design Metrics

Metrics Label	Description
Task Manager Custom Reports	Total number of custom reports
Task Manager Global Integration Tokens	Total number of global integration tokens
Note: * 0 or NA if no parent templates	

Table 12-7 Task Manager Runtime Metrics

Metrics Label	Description
Task Manager Schedules	Total number of schedules
Task Manager Active Schedules	Number of open or closed schedules
Task Manager Schedule Tasks	Number of tasks in all schedules
Task Manager Tasks in Active Schedules	Number of tasks in active schedules
Task Manager Manual Tasks in Active Schedules	Number of tasks in an active schedule from custom task types that are not associated with an integration
Task Manager Open Tasks in Active Schedules	Number of tasks in Open status in active schedules
Task Manager Closed Tasks in Active Schedules	Number of tasks in Closed status in active schedules
Task Manager Pending Tasks in Active Schedules	Number of tasks in Pending status in active schedules
Task Manager Error Tasks in Active Schedules	Number of tasks in Error status in active schedules
Task Manager Basic Tasks in Active Schedules	Number of Basic type tasks in active schedules
Task Manager Parent Tasks in Active Schedules	Number of Parent type tasks in active schedules
Task Manager UI Integrations Tasks in Active Schedules	Number of tasks in an active schedule from a custom task type associated with an end user integration
Task Manager Automated Tasks in Active Schedules	Number of tasks in an active schedule from a custom task type associated with an automated integration
Task Manager Event Monitoring Tasks in Active Schedules	Number of tasks in an active schedule from a custom task type associated with an event monitoring integration
Task Manager New Tasks in 1 Day	Number of new tasks in schedules created in the last day
Task Manager Opened Tasks in 1 Day	Number of tasks, including reopened tasks, that were set to Open status in the last day
Task Manager Closed Tasks in 1 Day	Number of tasks that were set to Closed status in the last day
Task Manager New Tasks in 30 Days	Number of tasks created in schedules in the last 30 days
Task Manager Opened Tasks in 30 Days	Number of tasks, including reopened tasks, that were set to Open status in the last 30 days
Task Manager Closed Tasks in 30 Days	Number of tasks that were set to Closed status in the last 30 days
Task Manager References	Total number of uploaded files
Task Manager References By Used Size in MB	Size, in MB, of all uploaded files

Table 12-7 (Cont.) Task Manager Runtime Metrics

Metrics Label	Description
Task Manager Average Duration of Closed Tasks in 30 Days	Average duration, in days, between the open and close date for tasks that were manually closed in the last 30 days * (see Note)
Task Manager Manually Closed Tasks in 30 Days	Number of tasks without associated integration or with URL integration only that were closed in the last 30 days
Task Manager Percentage of Manually Closed Tasks in 30 Days	Percentage of tasks without associated integration or with URL integration only that were closed in the last 30 days * (see Note)
Task Manager Percentage of Late Tasks in 30 Days	Percentage of manually closed tasks late for anyone in the workflow in the last 30 days * (see Note)
Task Manager Percentage of Rejected Tasks in 30 Days	Percentage of manually closed tasks with at least one rejection in the last 30 days * (see Note)
Task Manager Task Types Used in Active Schedules	Number of unique task types associated with tasks in active schedules
Task Manager Open Alerts	Total number of alerts in an Open status
Task Manager New Alerts in 1 Day	Number of new alerts created in the last day
Task Manager Closed Alerts in 1 Day	Number of alerts that were set to Closed status in the last day
Task Manager New Alerts in 30 Days	Number of new alerts created in the last 30 days
Task Manager Closed Alerts in 30 Days	Number of alerts that were set to Closed status in the last 30 days
Task Manager New Task Alerts in 30 Days	Number of new Alerts associated with tasks in the last 30 days
Task Manager Closed Task Alerts in 30 Days	Number of alerts associated with tasks that were set to Closed status in the last 30 days
Task Manager Pending Jobs in 1 day	Total number of Task Manager jobs that entered pending status in the last 24 hours due to conflicts.
Task Manager Pending Jobs in 30 days	Total number of Task Manager jobs that entered pending status over the past 30 days.
Note: * 0 if no manually closed tasks in the last 30 days	

Most Recent Metadata Validation Errors and Warnings

This table indicates the validation errors and warnings (generally displayed in the Validate Metadata screen) from the newest Financial Consolidation and Close metadata validation within the last 24 hours.
The title of this table indicates the time when you ran metadata validation, which may be different from the time at which the Activity Report was created.

Most Recent Metadata Validation Errors and Warnings (14:52:45)

Type	Dimension	Member Name	Cube Name	Validation Error
Error	Account	Statistical	Consol	The consol operator for all children of the dimension name should be Ignore or Never.
Error	Account	FX Exposure	Rates	The consol operator for all children of the dimension name should be Ignore.
Error	Account	2381		Account consol operator should be addition based on parent and child account types
Error	Account	2980		Account consol operator should be addition based on parent and child account types
Error	Account	2130		Account consol operator should be addition based on parent and child account types
Error	Account	Investment Detail		Account consol operator should be subtraction based on parent and child account types
Error	Account	1730		Default data storage should match with Consol cube data storage.
Error	Account	1730	Consol	Level 0 members should not be Dynamic Calc without member formulas.
Error	Account	1740		Default data storage should match with Consol cube data storage.
Error	Account	1740	Consol	Level 0 members should not be Dynamic Calc without member formulas.
Error	Account	7230	Consol	Level 0 members should not be Dynamic Calc without member formulas.
Error	Account	3500		Default data storage should match with Consol cube data storage.
Error	Scenario	ActualLYRate	Consol	The consol operator for all children of the dimension name should be Ignore or Never.
Error	Scenario	ActualLYRate	Rates	The consol operator for all children of the dimension name should be Ignore.
Error	Scenario	ActualBudRate	Consol	The consol operator for all children of the dimension name should be Ignore or Never.
Error	Scenario	ActualBudRate	Rates	The consol operator for all children of the dimension name should be Ignore.
Error	Scenario	Plan	Consol	The consol operator for all children of the dimension name should be Ignore or Never.
Error	Scenario	Plan	Rates	The consol operator for all children of the dimension name should be Ignore.
Error	Scenario	Forecast	Consol	The consol operator for all children of the dimension name should be Ignore or Never.
Error	Scenario	Forecast	Rates	The consol operator for all children of the dimension name should be Ignore.

Consolidation and Translation Jobs Statistics

Financial Consolidation and Close allows you to enable consolidation rules logging to identify and troubleshoot issues related to consolidation and close performance. By enabling consolidation rules logging, you generate the consolidation performance diagnostics logs that provide detailed insights into system behavior.

Top 5 Consolidation and Translation Jobs Detail by Duration

The **Top 5 Consolidation and Translation Jobs Detail by Duration** table presents key information from the consolidation performance diagnostics logs to help troubleshoot consolidation issues. Specifically, it reports on up to five jobs that consume the most processing time. For each job, the table identifies:

- The **rule template** that accounts for the majority of processing time
- The **number of entities** processed by each rule

Top 5 Consolidation and Translation Jobs Detail by Duration

Duration (HH:MM:SS)	CPU Time (HH:MM:SS)	Start Time	Job Type	Job ID	Period	Rule Template	Template Type	Level	Number Entities	Top 10 Entities-Duration more than 1 Sec
00:06:13	00:31:55	08:34:20	FORCECONSOLIDATE	429830	May	Insertion rule - FCCS_30_After Opening Balance Carry Forward_Translated	Insertion Rules	0	101	[AN10CONS].AN08]]: 20s, AN00CONS].AN02]]: 20s, 11CLCONS].AN21]]: 20s AN24CONS].AN16]]: 20s, Negocio_Local].11CL]]: 20s, ...See More
00:05:56	00:14:02	08:34:47	FORCECONSOLIDATE	429830	May	Insertion rule - FCCS_60_Final Calculations_Consolidated	Insertion Rules	0	101	[AN00CONS].51PE]]: 10s, AN10CONS].AN10]]: 9s, AN10CONS].AN06]]: 9s, AN00CONS].AN06]]: 9s, AN00CONS].AN08]]: 9s, AN10CONS].AN19]]: .... See More
00:05:57	00:09:33	08:34:39	FORCECONSOLIDATE	429830	May	Insertion rule - FCCS_40_Final Calculations_Translated	Insertion Rules	0	101	[AN10CONS].AN10]]: 6s, AN10CONS].AN06]]: 6s, AN00CONS].AN06]]: 6s, AN00CONS].AN08]]: 6s, AN10CONS].AN19]]: 6s, AN10CONS].AN02]]: .... See More
00:06:01	00:05:24	08:34:14	FORCECONSOLIDATE	429830	May	Insertion rule - FCCS_10_After Opening Balance Carry Forward_LocalCurrency	Insertion Rules	0	101	[AN10CONS].AN10]]: 3s, AN10CONS].AN02]]: 3s, AN10CONS].AN19]]: 3s, AN00CONS].AN08]]: 3s, AN10CONS].AN08]]: 3s, AN00CONS].AN00]]: .... See More

The Duration column in this table indicates how long a calculation takes. However, because of multiple cores and parallelism, duration may not indicate the actual processing cost (in time taken), which is indicated by the CPU Time column. For example, if the Duration is 10 minutes, the CPU Time is only one minute if 10 cores are used for processing.

Always start by looking at the Duration column, which matches the visual data in logs and tables. However, to identify processing bottlenecks, check the CPU Time column, which is the

true measure of a slow operation. Any row in this table with a high CPU time compared to other rows is a candidate for further optimization.

Reports and Books Execution Statistics

Activity Report taken from Narrative Reporting environments includes the Narrative Reporting Reports and Book statistics. For all other business processes, this report contains Financial Reporting statistics:

- Top 10 Longest Performing Book Generations Over 1 Min
  This table lists the top 10 Narrative Reporting and Financial Reporting books that took over one minute to generate. For each book, this table lists the book name, the time spent on generating the book, the user who generated the book, and a breakdown of each activity in the book generation process. The Object column in the table contains details of output type, folder, book POV, and other metadata.

Top 10 Longest Performing Book Generations Over 1 Min

Duration (Min:Sec)	User	End Time (UTC)	Name	Object	Breakdowns (Min:Sec)
04:28	xxxxxxx@example.com	18:43:23	/book1	Output=HTML Folder=/ BookPOV={Vision:Plan1 metadata= {HSP_View=HSP_View; Entity=User Point of View for Entity;Product=Product}}	essbaseConnections=00:00 totalEssbaseTime=00:01 ExecBook=04:28 GetADMResults=00:01 mdxQueriesTime=00:00 ExecReport=04:28 DataQuery=04:23 mdxQueries=00:00
04:07	xxxxxxx@example.com	19:19:28	/book1	Output=HTML Folder=/ BookPOV={Vision:Plan1 metadata= {HSP_View=HSP_View; Entity=User Point of View for Entity;Product=Product}}	essbaseConnections=00:00 totalEssbaseTime=00:00 ExecBook=04:07 GetADMResults=00:00 mdxQueriesTime=00:00 ExecReport=04:07 DataQuery=04:06 mdxQueries=00:00

- Top 10 Longest Performing Report Generations over 1 Min.
  This table lists the top 10 Narrative Reporting and Financial Reporting reports that took over one minute to generate. For each report, this table lists the report name, the time spent on generating the report, the user who generated the report, and a breakdown of each activity in the report generation process. The Object column in the table contains details of output type, folder, user POV, and other metadata.

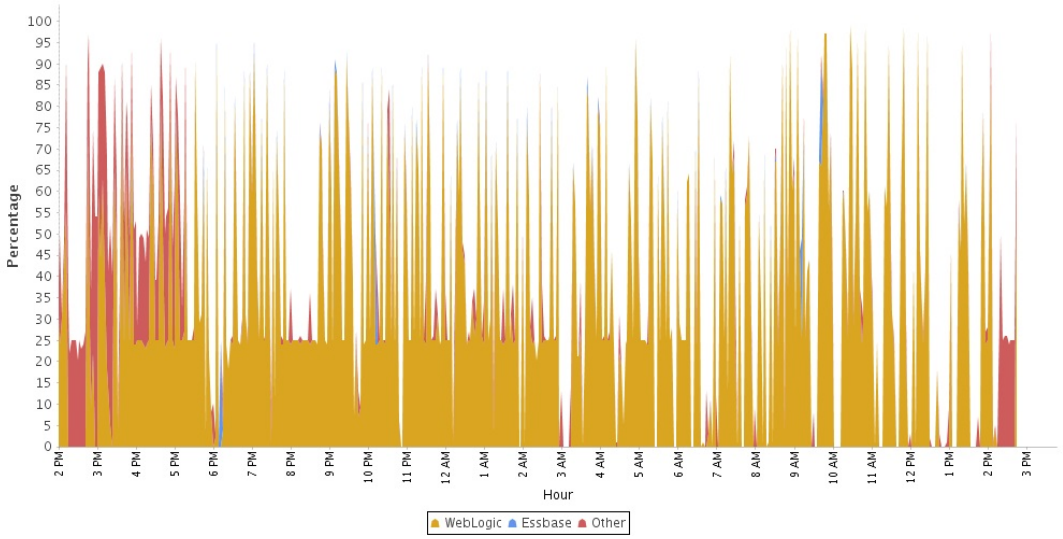
Top 10 Longest Performing Report Generations Over 1 Min

Duration (Min:Sec)	User	End Time (UTC)	Name	Object	Breakdowns (Min:Sec)
04:18	xxxxxxxx.example.com	18:49:34	/Report1	Output=HTML Folder=/ UserPOV={Vision:Plan1 metadata= {HSP_View=HSP_View; Product=Product}}	GetADMResults=00:00 DataQuery=04:18
04:14	xxxxxxxx.example.com	18:51:15	/Report1	Output=HTML Folder=/ UserPOV={Vision:Plan1 metadata= {HSP_View=HSP_View; Product=Product}}	essbaseConnections=00:00 totalEssbaseTime=00:00 GetADMResults=00:00 mdxQueriesTime=00:00 DataQuery=04:13 mdxQueries=00:00

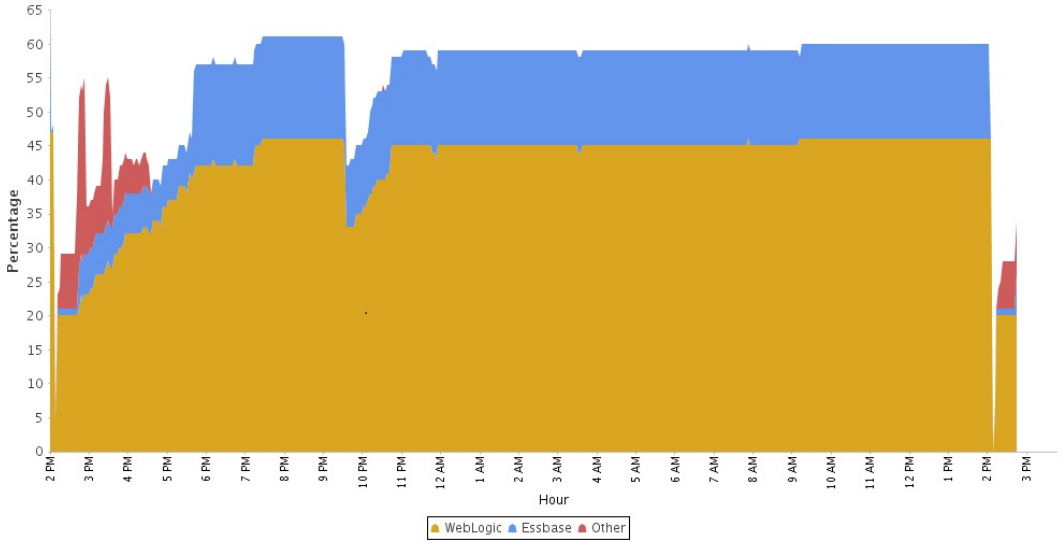
CPU and Memory Usage Statistics

The following information on CPU and memory usage is available:

- CPU usage for Oracle Essbase and application server.



- Memory usage for Essbase and application server.



Browser, Smart View, and Excel Usage Information

The following information is available:

- Oracle Smart View for Office versions being used and the number of users who used them.
- The 10 most active Smart View users who did not use the current version of Smart View.
- Top 10 users who used older versions of Smart View.
- 10 Most Active Smart View users on Older Versions of Microsoft Excel
- Microsoft Excel Versions in use and the number of users who used them.
- The versions of the browsers that were used to access the service and the number of users who used them.

- Unsupported browser versions and the number of users who used them.

Usage - EPM Automate

The Activity Report table displays the EPM Automate version in use and the number of users utilizing it.

EPM Automate Versions in Use

EPM Automate Version	Users
24.10.22	1

Using Access Logs to Monitor Usage

Access Log, which helps Service Administrators understand application usage by each active user, is automatically generated during the daily maintenance of the environment.

The Access Log contains information on users who logs into the environment directly or by using tools such as EPM Automate.

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management retain Access Logs for the last 60 days only. Oracle recommends that you download and create backup copies on a local computer to analyze them for historical trends. The Access Log for the day will not be available if you cancel the daily maintenance of the environment.

Viewing and Downloading Activity Reports and Access Logs

> **Note**
>
> - The information in this section is not applicable to Narrative Reporting.
> - The JSON version of the Activity Report is not accessible from the service. Use the `downloadfile` EPM Automate command to download it.

To view and download Activity Reports and Access Logs:

1. Access the service. See Accessing Cloud EPM and Cloud EDM Environments.
2. Perform an action. Choose from:
   - **Profitability and Cost Management only:** Click **Application**, then **Application**, and then **Performance**.
   - **Account Reconciliation only:** Click **Tools**, and then **Service Activity**.
   - **Oracle Fusion Cloud Enterprise Data Management only:** Click **Reports**, and then **Activity Reports**.
   - **Other services:** Click **Application**, then **Overview**, and then **Activity Reports**.
3. Perform an action. Choose from:
   - To open an activity report, click **View** under **Activity Report** in the row that indicates the day for which you want to view the report. Select a tab for quick access to relevant information. See Using the Activity Report.

Activity Reports created during Provide Feedback uses `Feedback` as the prefix.

- To view and download an access log, click **Download** under **Access Log** in the row that indicates the day for which you want to download the log.

Automating Activity Report and Access Log Download

Use the downloadFile EPM Automate command to download activity reports and access logs to a local computer if you need them for audit purposes.

Oracle provides you a script that demonstrates how to use the `downloadfile` command to automate file download process. For detailed information, see these topics in *Working with EPM Automate*:

- Automate Activity Report Downloads to a Local Computer
- Download Access Logs from an Environment
- Automating Script Execution
- Installing EPM Automate
- Running EPM Automate

Using the Role Assignment Report to Monitor Users

The Role Assignment Report is generated from Access Control, EPM Automate, and REST API to:

- Identify users who are assigned predefined roles that enable them to access an environment.
  The report lists all the predefined roles assigned to the user.
- Display the number of users of an environment and the application-level role assignment of each user.

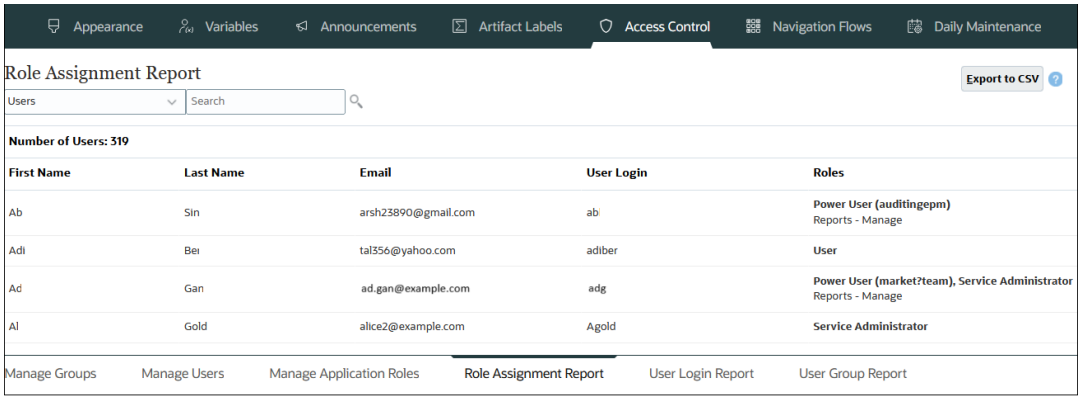
> **Note**
>
> If a predefined role is assigned to an IDCS group, the Role Assignment Report will show that predefined role assigned directly to all users in that group.

Viewing the Role Assignment Report in Access Control

To view the Role Assignment report for an environment:

1. Access the service as a Service Administrator. See Accessing Cloud EPM and Cloud EDM Environments.
2. On the Home page, Click **Tools**, and then **Access Control**.
3. Click **Role Assignment Report**.

   The Role Assignment Report, which shows the number of authorized users, their roles, and how those roles are granted, is displayed.



Using a Script to Automate the Process

Using EPM Automate, you can automate the process of creating the Service Administrator Report and counting the number of users who are assigned to predefined roles in an environment. See "Scenario 12: Counting the Number of Users Assigned to Roles" in *Working with EPM Automate*.

Monitoring Environments Using Oracle Cloud Console

The Oracle Cloud Console dashboard can be used to monitor the Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments.

The details regarding the Cloud EPM and Cloud EDM environments are presented in the activity report. See Information About Your Environment.

Monitoring Metrics

To monitor the number of unique users, average user interface response time, and data size of your Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments, see the activity report information:

- User Information
- Interface Usage and Response Data
- Customer Data on Disk in GB in Application Size.

Managing and Viewing Announcements

Oracle Cloud Console announcements communicate important updates on service status. You can view a list of current and past announcements. To receive announcements via email or other delivery methods, you can manage tenancy administrator email preferences or set up announcement subscriptions. In this section:

- Enabling Announcements
- Viewing Announcements
- Creating Announcement Subscription

Enabling Announcements

By default, only Cloud Account Administrators and Identity Domain Administrators can view announcements. Service Administrators of individual environments must be assigned the appropriate policies to view them.

For environments migrated from My Services to the Oracle Cloud Console, Service Administrators are added to the *<service_name>_Console_Upgrade_Service_Admin_Group* and the *<service_name>_Console_Upgrade_Service_Admin_Group_Policy* is automatically assigned to this group. This gives them the necessary permission to view the announcements. For example, <service_name> could be Planning.

For newly created environments, Identity Domain Administrators can assign these policies by adding Service Administrators to groups that are associated with specific policies. To enable announcements:

1. Sign in to the Oracle Cloud Console.
2. (Optional) If needed, create the users and groups to whom you want to assign policies. See:
   a. Creating User
   b. Creating IDCS Groups
3. Create a policy for the selected group of users assigned as Service Administrators. See Creating Policies for Users and Groups. In **Policy Builder**, enter the following policy statements:

> **Note**
>
> Be sure to replace *GROUP_NAME* with the name of the group to which you want to apply the policy

- To view the announcement:

```
Allow group <identity-domain-name>/GROUP_NAME to read announcements in
tenancy
```

- To manage the announcement:

```
Allow group <identity-domain-name/GROUP_NAME to manage announcement-
subscriptions in tenancy
Allow group <identity-domain-name/GROUP_NAME to manage ons-topics in
tenancy
```

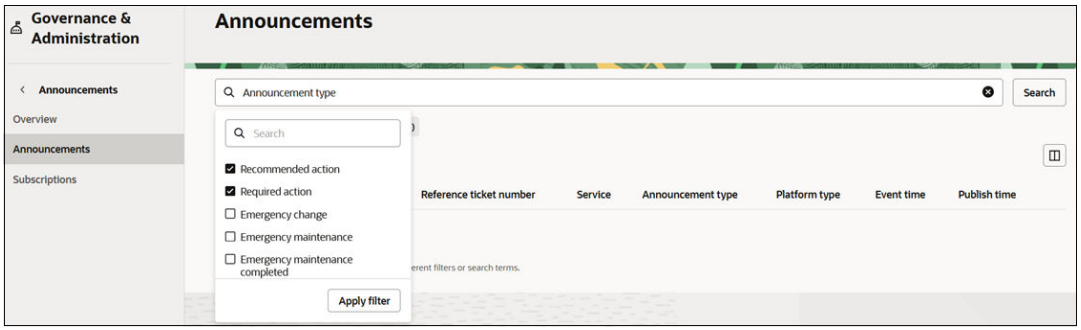
Viewing Announcements

Once the Announcements are enabled, you can view a list of all announcements when you want to know what announcements you have for a particular compartment, including the root compartment. See Viewing a List of All Announcements in *Oracle Cloud Infrastructure* documentation.

To view an announcement:

1. Click  (Announcements) at the top right corner of the console.

2. Click **Announcements** on the left pane.
3. The **Announcements** page displays all announcements for the selected compartment. Use the **Compartment** filter to switch compartments.
4. You can filter the list of announcements for the following:
   - Select **Announcement**, and then enter a full or partial announcement title.
   - Select **Read status**, and then select one or more statuses.
   - Select **Reference ticket number**, and then enter a reference ticket number.
   - Select **Service**, and then select one or more services.
   - Select **Announcement type**, and then select one or more announcement types
   - Select **Action type**, and then select one or more action types.
   - Select **Platform type**, and then select one or more platform types.
   - Select **Event time**, and then enter a start date, start time, end date, and end time. Or, you can select one of the preset time ranges, up to the last year.
   - Select **Publish time**, and then enter a start date, start time, end date, and end time. Or, you can select one of the preset time ranges, up to the last year.
5. Click **Apply filter**. The following image displays how to search and select Announcement types to filter announcements.



6. (Optional) To clear filters, perform one of the following actions, depending on what's available:
   - To clear an individual filter, select the **X** next to the filter name.
   - To clear all filters on the list of announcements, select **Reset**.

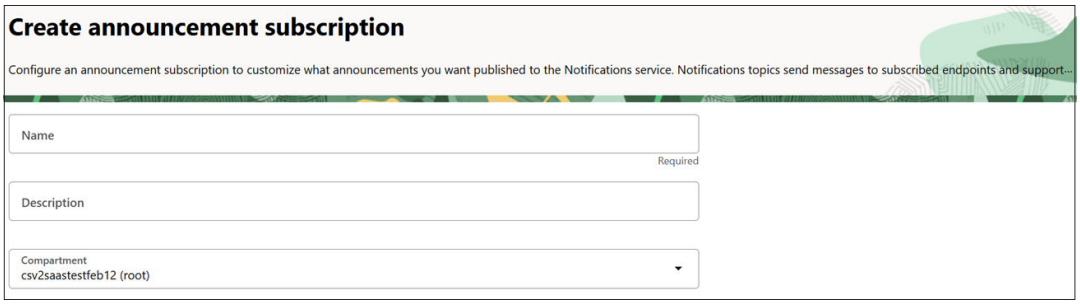
Creating Announcement Subscription

To receive only relevant announcements, create an announcement subscription. This allows you to set filters to define the criteria announcements must meet before they're sent to subscribers. When creating an announcement subscription, you'll also define an Oracle Cloud Infrastructure Notifications topic, which serves as the communication channel for publishing filtered announcements.A Notifications topic is a communication channel for sending messages to its subscriptions. A topic can have zero, one, or multiple subscriptions that are notified whenever a message is published to a topic. The announcements then arrive to you and other recipients, as appropriate, at the delivery endpoints configured in the Notifications topic.

For environments migrated from My Services to the Oracle Cloud Console, Service Administrators are automatically added to subscription *migrated_announcement_subscription_<servicename>_** where <*service_name*>refers to

business processes like Planning or Account Reconciliation and * is a sequential number for the subscriptions. Each subscription can have a maximum of 10 endpoints, such as email addresses.
To create a new announcement subscription:

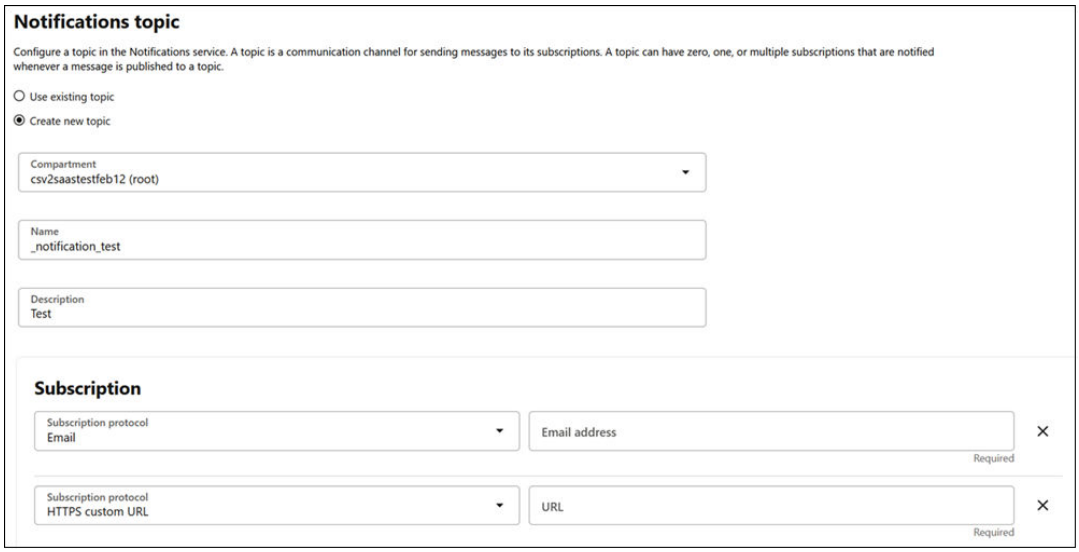
1. Click (Announcements) at the top right corner of the console.
2. Click **Subscriptions** on the left pane.
3. On the Subscriptions list page, click **Create announcement subscription**.
4. Enter a **Name** and **Description** for the announcement.
5. Select the **Compartment** where you want the subscription created.



6. Under **Subscription type**, choose one of the following:
   - To publish all announcements, select **All announcements** and proceed to configure the Notifications topic.
   - To publish only announcements that meet your filter criteria, select **Selected announcements only**.
7. If you selected **Selected announcements only**, under Filter group, select **Filter group name**, and then enter a name for the filter.
8. Under Filters, select **Type**, and then choose the **Value** options to filter by type.

> **Note**
>
> You can only have one filter of each type within a filter group. To add additional filters, select **+ Another filter**. Note that filters based on resource OCIDs cannot be combined with other filter types in the same group.

9. (Optional) To combine different filters for specific criteria, click **Add filter group** and repeat the steps above.
10. Under Display preferences, select your preferred **Time zone** for announcement time stamps.
11. Under Notifications topic, choose:
    a. **Use existing topic** to select a topic from the current compartment or choose a topic from a different compartment if necessary. Skip to step 13.
    b. **Create new topic** to set up a new topic.
12. If you choose to create a new topic, enter the **Compartment**, **Name**, and **Description**.
13. Select the **Subscription protocol** for the subscription endpoints and provide the necessary information based on the protocol.
14. To add more subscription protocols, click **Add Subscription**.



15. Finally, click **Create** to finish setting up the subscription.

A

Frequently Asked Questions

This section compiles Frequently Asked Questions (FAQs) with answers, addressing topics related to setting up, securing, and monitoring Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management environments. It also includes links to FAQs for Cloud EPM business processes and Cloud EDM in their respective administration guides.

Table A-1 FAQs in Cloud EPM

Topic	FAQs
Authenticating and Authorizing Access to Environments	• How do I set up authentication with OAuth 2? • Does Cloud EPM or Cloud EDM require new certificates to be installed if a connection to Oracle Fusion Cloud is configured and the Fusion certificates are updated? • How do I reset users' passwords? • How to force user synchronizing within an application? • Does Cloud EPM and Cloud EDM support DKIM (DomainKeys Identified Mail) for email authentication? • I am getting emails from no-reply@oracle.com. How to change From address in email? • How do I create or remove EPM groups? • How do I add or remove users from EPM group?
Working with subscriptions	• Why am I unable to create Oracle Cloud account in MyServices? I am seeing the message: Account setup has been already initiated or canceled. Please wait for the activation e-mail • If I am transitioning from the Enterprise Data Management business process to Cloud EDM, can I set up the standalone environment on the same domain? • If I am transitioning from the Enterprise Data Management business process to Cloud EDM, can I set up the standalone environment on the same URL? • From a security perspective, can the same Identity domain and SSO be used when transitioning from the Enterprise Data Management business process in the EPM Enterprise Subscription to Cloud EDM ?
Compliance Reporting	• How can I obtain the SOC1 and SOC2 reports for Cloud EPM and Cloud EDM services? • Where can I learn about penetration (pen) testing and vulnerability testing?

Table A-1 (Cont.) FAQs in Cloud EPM

Topic	FAQs
Backup and Disaster Recovery	• How long does Oracle retain production and test backups, and how do I copy a backup snapshot to my environment? • How do I restore Cloud EPM and Cloud EDM environments? • What happens when Daily Maintenance is kicked off? • What disaster recovery options are available for Cloud EPM and Cloud EDM? • How can I set up backup and disaster recovery for my own Object Storage bucket?
Migrating Data to Environments	• How do I perform a Production-to-Test Data Migration? • How to resolve a cloning error?
Maintaining Environments	• How do I restart an environment? • How do I postpone the automatic monthly update of my environment?
Monitoring the Environments	How can I monitor application usage and performance in Oracle Cloud EPM?
Engaging Oracle support	How do I use the Provide Feedback feature to assist technical support when troubleshooting Cloud EPM and Cloud EDM services?
FAQs in EPM Platform	• Frequently Asked Questions in Smart View in *Smart View for Office User's Guide 24.100* • Frequently Asked Questions in *Administering Data Integration for Oracle Enterprise Performance Management Cloud*
FAQs in Cloud EPM Business Processes	• FreeForm Apps FAQ in *Administering FreeForm* • Frequently Asked Questions (FAQ) about Enterprise Profitability and Cost Management in *Administering and Working with Enterprise Profitability and Cost Management*
FAQs for Cloud EDM	Frequently Asked Questions in *Administering and Working with Enterprise Data Management*

> **Note**
>
> Find troubleshooting tips and information on common customer-reported issues with procedures to correct them and steps to make a request to Oracle in Oracle Enterprise Performance Management Cloud Operations Guide.

Authenticating and Authorizing Access to Environments

How do I set up authentication with OAuth 2?

You can use OAuth 2 access tokens to make REST API calls to Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management, and to use EPM Automate and the EPM Integration Agent to satisfy the requirement of avoiding the use of passwords in your environments. See:

- Using OAuth 2.0 Authorization Protocol with OCI in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Authentication with OAuth 2 - Only for OCI in *REST API for Enterprise Performance Management Cloud*

Does Cloud EPM or Cloud EDM require new certificates to be installed if a connection to Oracle Fusion Cloud is configured and the Fusion certificates are updated?

No, there is no need to install Fusion certificates on Cloud EPM and Cloud EDM.

How do I reset users' passwords?

The Identity Domain Administrator has the capability to reset the Cloud EPM or Cloud EDM user's password. When the password reset is successful, the system automatically generates a new password and mails this temporary password directly to the user. Users are required to change the temporary password the next time they sign in. You can reset the password using IAM Interface.

How to force user synchronizing within an application?

Sometimes, a predefined role assignment may not take immediate effect in an environment. To address this, follow the guidelines in Role Assignment Is not Immediately Reflected in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Does Cloud EPM and Cloud EDM support DKIM (DomainKeys Identified Mail) for email authentication?

Cloud EPM and Cloud EDM on OCI (Gen2) environments supports DKIM (DomainKeys Identified Mail). For details, see DKIM Support.

I am getting emails from no-reply@oracle.com. How to change From address in email?

To change the sender, see Requesting Custom Sender Email Address for OCI in *Oracle Enterprise Performance Management Cloud Operations Guide*

How do I create or remove EPM groups?

To create EPM groups, see:

- createGroups in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Add Groups in *REST API for Enterprise Performance Management Cloud*
- Creating EPM Groups in *Administering Access Control for Oracle Enterprise Performance Management Cloud*

To remove EPM groups, see:

- deleteGroups in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Remove Groups in *REST API for Enterprise Performance Management Cloud*
- Deleting EPM Groups in *Administering Access Control for Oracle Enterprise Performance Management Cloud*

How do I add or remove users from EPM group?

To add users to a group, see:

- addUsersToGroup in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Add Users to a Group in *REST API for Enterprise Performance Management Cloud*
- Assigning a User to Many Groups in *Administering Access Control for Oracle Enterprise Performance Management Cloud*

To remove user from a group, see:

- removeUsersFromGroup in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Remove Users from a Group in *REST API for Enterprise Performance Management Cloud*
- Assigning a User to Many Groups in *Administering Access Control for Oracle Enterprise Performance Management Cloud*

Working with Subscriptions

Why am I unable to create Oracle Cloud account in MyServices? I am seeing the message: `Account setup has been already initiated or canceled. Please wait for the activation e-mail`

On purchasing Oracle Fusion Cloud Enterprise Performance Management or Oracle Fusion Cloud Enterprise Data Management subscription as a first-time customer), Oracle sends you, the person designated as the initial contact (whose email ID was provided while ordering the subscription), an email that identifies the steps to activate and provision it. For more information, see The Subscription Activation Email. Follow instructions for first-time customers.

If I am transitioning from the Enterprise Data Management business process to Cloud EDM, can I set up the standalone environment on the same domain?

Yes, the standalone Cloud EDM can be set up on the same domain as the existing Enterprise Data Management business process, provided that both the cloud account and identity domain are part of the same primordial stripe.

If I am transitioning from the Enterprise Data Management business process to Cloud EDM, can I set up the standalone environment on the same URL?

No, this is not possible unless the current environment is moved to a new location. The process involves resetting the environment, creating a new Cloud EDM subscription with the original Cloud EPM Enterprise Data Management business process name, and then performing the clone.

For example, if the current Oracle cloud account has the Enterprise Data Management business process name as `edm1/edm1-test`, the following steps must be taken:

1. Move the app and data to a temporary holding location, such as `epme3/epm3-test`.
2. Clone the environment from `edm1/edm1-test` to `epme3/epm3-test`.
3. Delete the original environment, `edm1/edm1-test`.
4. Once the deletion is processed, create a new Cloud EDM environment within the Oracle cloud account and assign the service name `edm1`.
5. After the new Cloud EDM environment is created, clone the environment from `epme3/epm3-test` back to `edm1/edm1-test`.

This double clone process is only necessary if you wish to retain the same URL and business process name.

From a security perspective, can the same Identity domain and SSO be used when transitioning from the Enterprise Data Management business process in the EPM Enterprise Subscription to Cloud EDM ?

Yes, the security setup for Cloud EDM can use the same identity domain and SSO as the existing Enterprise Data Management environment. However, you will need to assign access within the Oracle Identity Cloud to ensure the appropriate permissions are set up.

Compliance Reporting

How can I obtain the SOC1 and SOC2 reports for Cloud EPM and Cloud EDM services?

You can access these reports in the Oracle Cloud Console. See Accessing Compliance Reports.

Where can I learn about penetration (pen) testing and vulnerability testing?

Review this topic for helpful information: Periodic Penetration Testing and Ethical Hacking to Identify and Fix Vulnerabilities.

Backup and Disaster Recovery

What is the process to take backup of Cloud EPM and Cloud EDM environments?

Each day, at the scheduled maintenance time of the environment, Oracle creates a maintenance snapshot called the Artifact Snapshot, which includes a backup of the existing artifacts and data. See Overview of the Maintenance Snapshot.

How long does Oracle retain production and test backups, and how do I copy a backup snapshot to my environment?

Oracle retains the production and test environment snapshots for 60 days. Use the listBackups and restoreBackup EPM Automate commands to check for and copy available backup snapshots to your environment. Alternatively, you can use the List Backups and Restore Backup REST APIs.

For more details, see Archival, Retention, and Retrieval of Daily Snapshots.

How do I restore Cloud EPM and Cloud EDM environments?

You can use the maintenance snapshot to recover artifacts and data from a previous day. If you want to restore from the previous day, the Artifact Snapshot can be used. Otherwise, you'll need to obtain the maintenance snapshot for the specific day you wish to restore. Once you have the correct snapshot, you can copy it to the environment and import from it. See:

- Backing Up and Restoring an Environment Using the Maintenance Snapshot
- restoreBackup and importSnapshot commands in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*.

What happens when Daily Maintenance is kicked off?

Find information on Daily Maintenance in Daily Maintenance Operations.

What disaster recovery options are available for Cloud EPM and Cloud EDM?

Oracle Fusion Cloud Enterprise Performance Management and Oracle Fusion Cloud Enterprise Data Management provide self-service options to restore your environments to a working state. See:

- Overview of the Maintenance Snapshot
- Replicating an EPM Cloud Environment in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Backup and Disaster Recovery for the Object Storage Bucket

How can I set up backup and disaster recovery for my own Object Storage bucket?

If you use Object Storage to store snapshots in a Cloud EPM or Cloud EDM environmment, or to store attachments for Account Reconciliation, Financial Consolidation and Close, Tax Reporting, or Enterprise Profitability and Cost Management, you can configure a replication bucket as a backup. This setup ensures continuity in case the primary bucket becomes temporarily unavailable.

Below are the keys steps to setup backup and disaster recovery for an Object Storage bucket:

1. **Create the primary bucket:**
   a. Create the main Object Storage bucket in a selected region.
   b. Configure it in your Cloud EPM or Cloud EDM environmment to store snapshots or attachments.

> **Note**
>
> For instructions on how to create a bucket and store an object in the bucket, see Putting Data into Object Storage.

2. **Set up a replication bucket:**
   a. Create a second bucket in a different OCI region.
   b. Configure replication from the primary bucket to this replication bucket.

> **Note**
>
> For task documentation related to buckets, see Object Storage Buckets, Object Storage Replication, and Object Storage Data Retention Rules.

3. **In case of a disaster, if the primary bucket is affected, switch to the replication bucket:**
   a. Make the replication bucket writable.
   b. Update the Cloud EPM or Cloud EDM configuration to use the replication bucket as the new main bucket.

> **Note**
>
> The snapshots or attachments will now be stored in replication bucket.

4. **Once primary bucket is back online, to restore the original setup after recovery:**
    a. Reconfigure Cloud EPM or Cloud EDM environment to use primary bucket as the main bucket again.
    b. Copy any delta (new or changed) files from replication bucket back to primary bucket .
    c. Re-establish replication from the primary bucket to the replication bucket.

Migrating Data to Environments

How do I perform a Production-to-Test Data Migration?

You migrate data from production to test using the **Clone** feature. See:

- Cloning EPM Cloud Environments in *Administering Migration for Oracle Enterprise Performance Management Cloud*.
- Alternatively, you can use the cloneEnvironment command in EPM Automate.
- You can also use the Clone an Environment REST API.

If you want to migrate only selected artifacts from production to test: you can go to Migration UI, select the individual artifacts, and export them from the production environment, then, you can copy that snapshot using `copysnapshotfrominstance` EPM Automate command. Once the snapshot is on the test environment, you can import it using Migration UI or `importsnapshot` EPM Automate command.

How to resolve a cloning error?

If you encounter an error while using the Clone Environment screen, the cloneEnvironment command in EPM Automate, or the Clone an Environment REST API, refer to the troubleshooting steps in Resolving Clone Environment Issues section of the *Oracle Enterprise Performance Management Cloud Operations Guide*.

How are data values stored in Essbase, and what causes it to load a value like ‘10’ as ’10.00000000001’?

Oracle Essbase represents cell values as IEEE double values. Doubles have a maximum of 15 significant digits of precision. Anything beyond the 15th digit is imprecise. For more information, see "Data Values in EPM Cloud" in About Essbase in Cloud EPM.

Maintaining Environments

How do I restart an environment?

To restart an environment, you can either use **resetService** EPM Automate command or **Restart the Service Instance** REST API. See:

- resetService in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Restart the Service Instance (v2) in *REST API for Enterprise Performance Management Cloud*

How do I postpone the automatic monthly update of my environment?

To postpone an automatic monthly update, you can use either the **skipUpdate** EPM Automate command or **skipUpdate** REST API. See:

- skipUpdate in *Working with EPM Automate for Oracle Enterprise Performance Management Cloud*
- Skip Updates (v2) in *REST API for Enterprise Performance Management Cloud*

For more information, see Requesting to Skip Automatic Updates for Environments in *Oracle Enterprise Performance Management Cloud Operations Guide*.

Monitoring the Environments

How do I monitor application performance in Oracle Cloud EPM?

You can monitor usage and performance through the **Activity Report**, which offers valuable insights into daily application usage and performance. It helps you assess key areas such as form activity, business rule execution, and calculations that may impact overall performance. These insights can guide you in optimizing your application design.

The Activity Report also enables you to:

- Understand usage patterns and user interactions
- Identify operations or requests that may impact performance
- Track changes in the application environment
- Investigate issues using graphical summaries and detailed data reports

For more information, see Using the Activity Report.

Engaging Oracle Support

How do I use the Provide Feedback feature to assist technical support when troubleshooting Cloud EPM and Cloud EDM services?

Click your user name (displayed at the right top corner of the screen), and then select **Provide Feedback**. For more information, see Submitting Information Using Provide Feedback.

> **Note**
>
> If you are a Service Administrator, including a maintenance snapshot can help technical support troubleshoot your service. In the Provide Feedback utility, expand **Confirm Application Snapshot submission**, and then enable the **Submit application.** This option is disabled if your organization enforces a policy that restricts Oracle's access to data, preventing Service Administrators from submitting the application snapshot to Oracle. It is also disabled in all restricted OCI regions (for example, regions in the OC2 and OC4 realms).