Oracle Fusion Cloud Financials

Getting Started with Your Financials Implementation

26C

Oracle Fusion Cloud Financials
Getting Started with Your Financials Implementation

26C

G56236-01

Author: Angie Shahi

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 Introduction

Overview of Implementing Oracle Financials Cloud

You can use the rapid implementation features to implement users, security, enterprise structures, banks, tax, ledgers, and financial subledgers. This document provides a high-level introduction to Oracle Financials.

> **Note:** This guide covers the basic requirements used to create an implementation project. The tasks presented in this document are intended for a quick introduction or pilot implementation. This document doesn't include all setup and security tasks that are appropriate for a complete implementation.

The rapid implementation setups for Financials include implementing:

- Users
- Enterprise structures
- Bank, branches, and bank accounts
- Tax
- Ledgers
- Business units
- Financial reporting
- Payables and payments
- Assets
- Expense reporting
- Receivables and payments

References to related help accompany each of the steps. Help and additional information are available from:

- Oracle Cloud Help Center (docs.oracle.com)
- Oracle Fusion Applications Help embedded in the applications

Overview of Oracle Financials Cloud

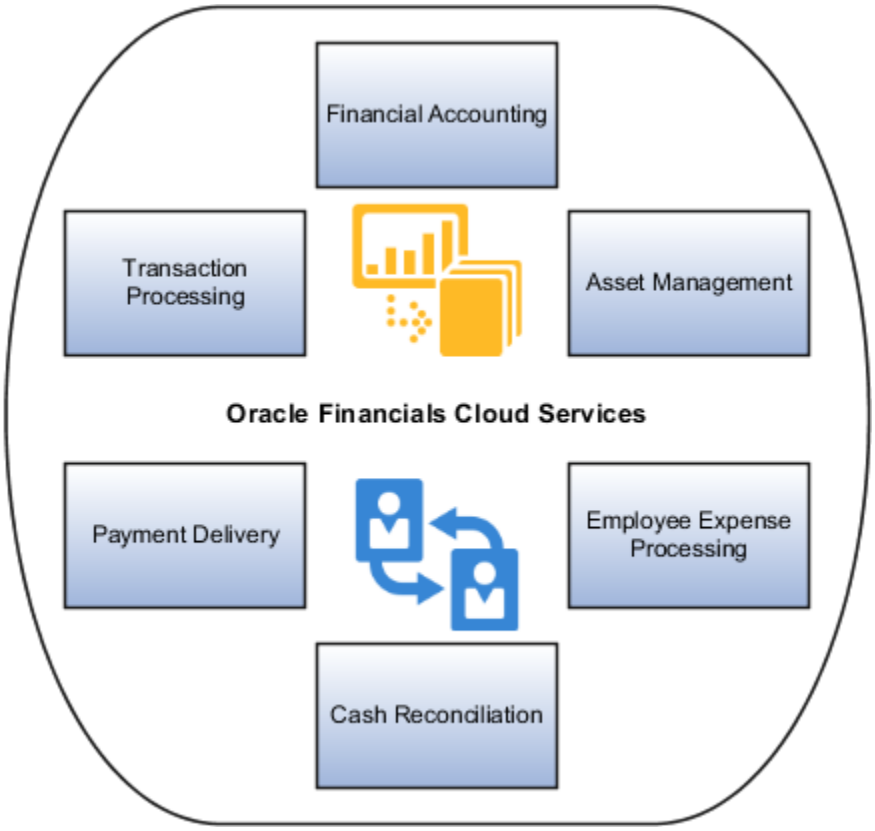
Oracle Financials delivers a complete solution that includes:

- General Ledger
- Intercompany Accounting
- Payables
- Receivables
- Payments
- Cash Management

- Tax
- Expenses
- Assets

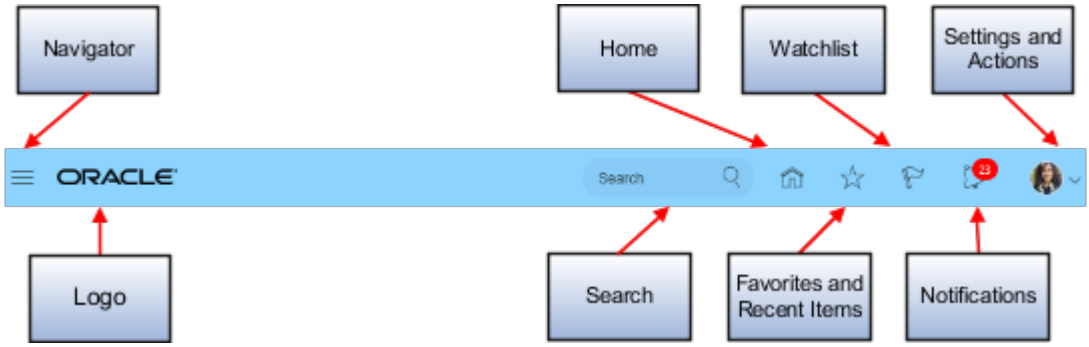
Use these applications with business intelligence, compliance reporting, and mobile data access for:

- Financial accounting
- Transaction processing
- Payment delivery
- Cash reconciliation
- Employee expense processing
- Asset management



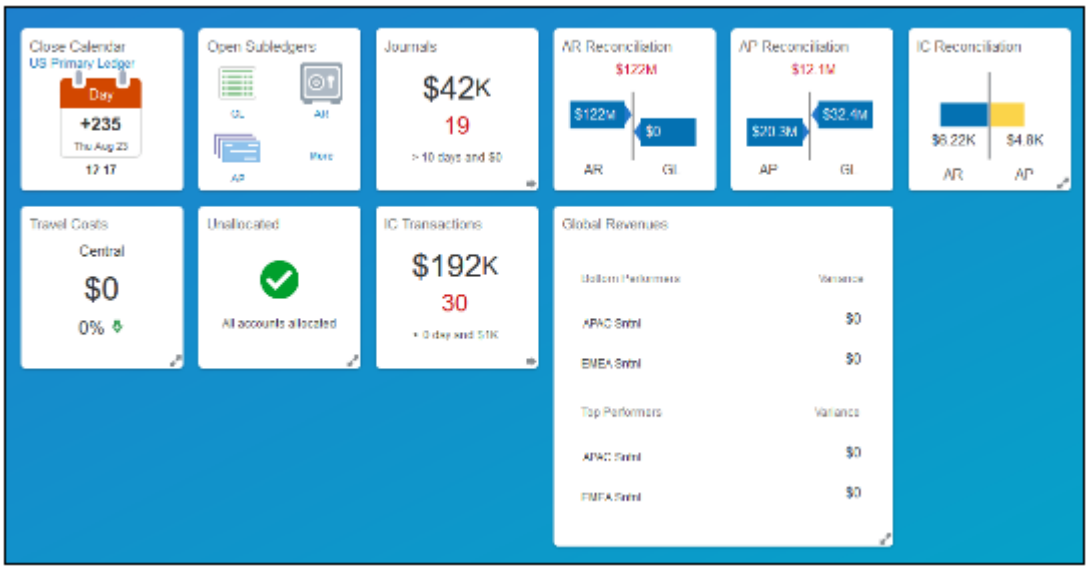
Access data through pages that contain:

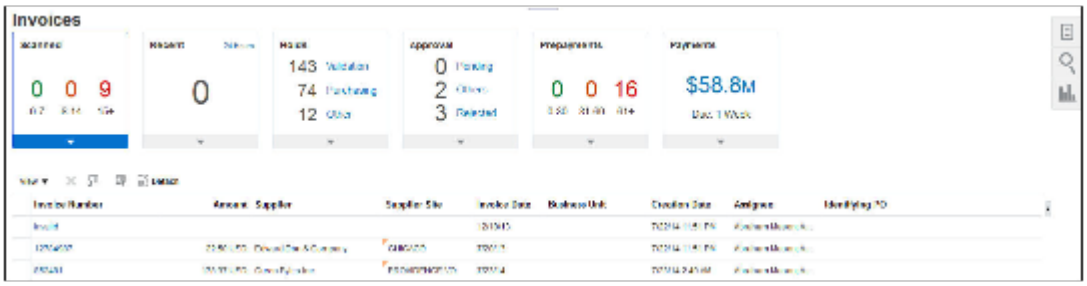
- Navigation tools in the global area of the Home page.



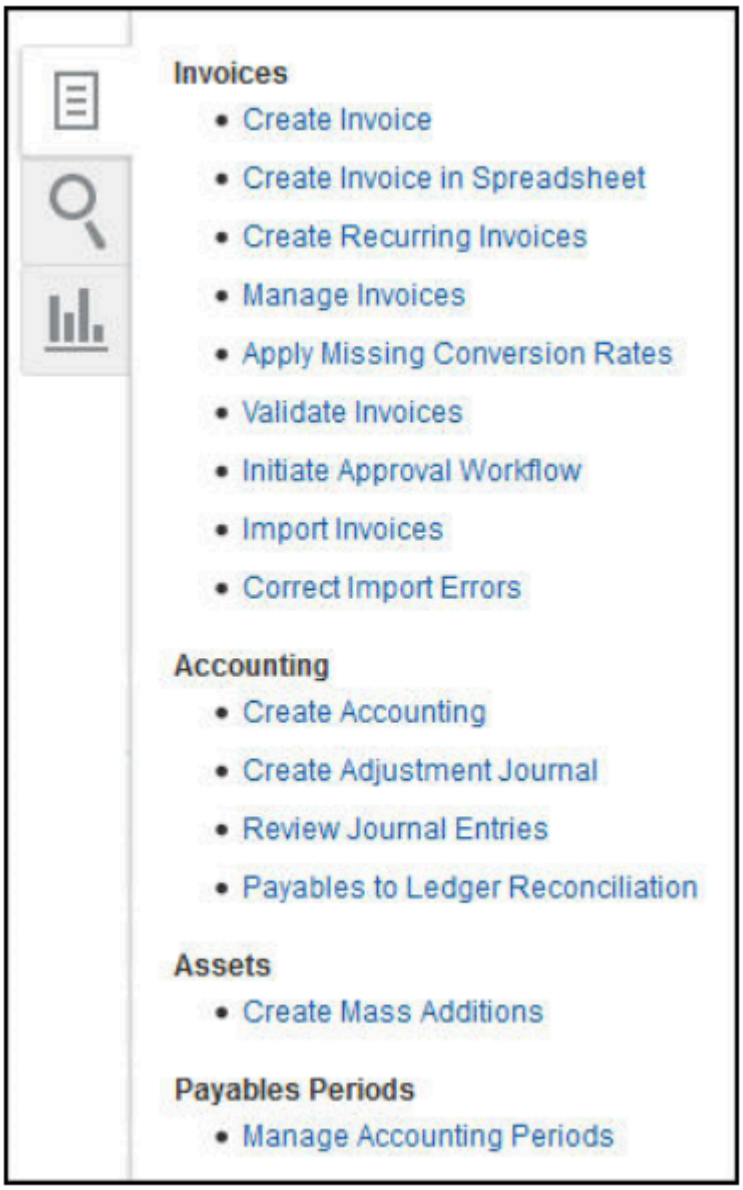
- Icons to navigate to pages.

- Infolets in an Infolets page or work area.

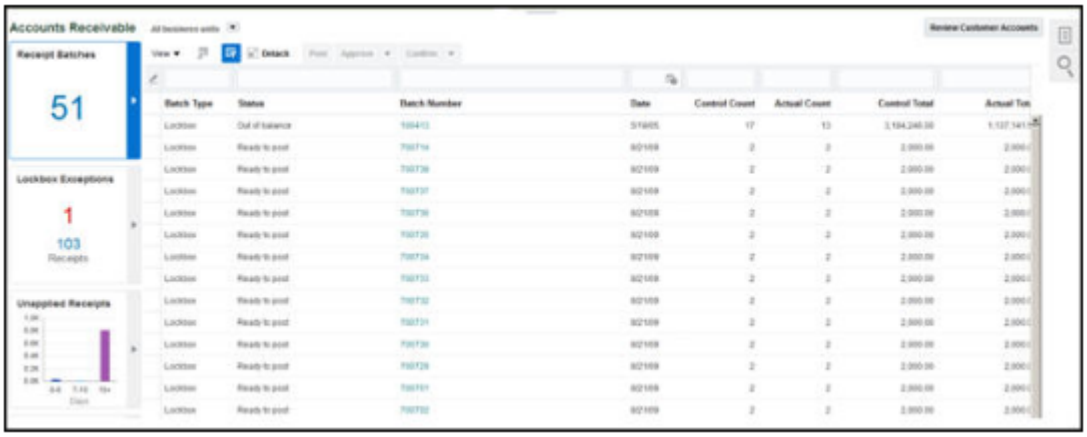




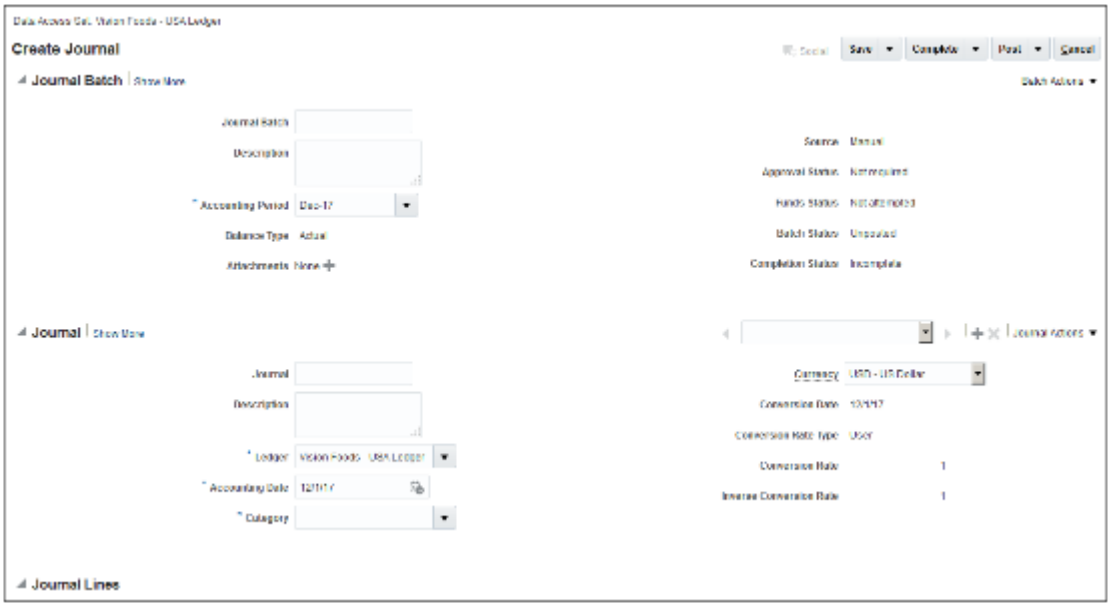
- Panel tabs for tasks, searching, and analytics accessed by icons on the page.



- Transaction details in a work area.



- Transaction details as a separate page.



From the application pages, access:

- **Embedded analytics**, which enables you to complete a transaction or analyze data.
- Interactive **infolets** and **work areas** to view:
  - Information summaries for a high-level overview.
  - Information monitoring and drill-down capability.
  - Transaction information that's central to one or more business processes.
  - Business intelligence content that's complementary to one or more business processes.
- **Real-time reporting** for:
  - Viewing reports and analytics for each individual work area.
  - Exploring predefined analyses.

- Creating and editing analyses from the **Reports and Analytics** panel tab or work area.
- Accessing the Oracle Business Intelligence (BI) Enterprise Edition through the **Reports and Analytics** panel tab. See the new objects and changes to existing objects that you made in Oracle BI Enterprise Edition, which are then available from Oracle Financials.
- Viewing and running financial reports from the Financial Reporting Center, which is a single point of entry for general ledger financial reporting functions. The Financial Reporting Center includes:
  - Tools to create and format financial reports, including Financial Reporting Studio and Workspace.
  - Live and interactive financial reports with multiple output options, including HTML, PDF, Excel, or Excel in Query Ready mode using Smart View Enabled formats.
  - Drill downs to underlying journals and subledger transactions with the Account Inspector.
  - Multiple reporting methods for ad hoc analysis, efficient monitoring, and tracking of key account balances in real time with the Account Monitor.

Overview of Using Infolets to Identify Issues and Prioritize Tasks

Use infolets to gain real-time insight into common financial activities and prioritize your daily activities. Understand your organization's status using graphs and indicators to focus on issues in general accounting and cash transactions.

This overview gives a brief outline of the General Accounting infolets and the tasks you can accomplish using them.

Navigate to the General Accounting Infolets page using the page control icons on the home page. You can perform the following activities using infolets:

- Configure individual infolets according to your financial specifications. For example, you can adjust the thresholds by flipping the infolet to expose the filtering criteria. When you flip the infolet back, the data now represents the new thresholds.
- Configure infolets in other ways to align with your business practices. For example, you can edit a title using the Actions icon on the infolet. You can also select what views you want to enable, such as a summary front and back view or an expanded view displaying additional details.
- Access underlying reports and pages from the information displayed on the infolet. For example, you can drill down to review the detailed information and make corrections on that same page, if necessary.
- Use the **Infolets Repository** to enable or disable individual infolets available to you. For example, you can deselect infolets that you don't need and when you go back to the infolets page, those infolets are hidden.

Overview of Using Work Areas to Streamline Business Processes

Use work areas to gain instant insight into your business and identify potential problems with processing transactions. Work areas are available in areas such as Accounts Payable Invoices, Accounts Receivable, Billing, Advanced Collections, and Fixed Assets.

Work areas can include the following:

- Infotiles
- Content area
- Actions toolbar
- Tasks panel tab
- Search panel tab
- Reports and Analytics panel tab

Infotiles

Infotiles summarize a high volume of transactional information. You can quickly identify potential problems and prioritize your daily activities by scanning the infotiles and accessing transaction details.

For example, select an infotile to display corresponding transactional information in the content area. You can also click links in the infotile to filter the records in greater detail in the content area.

Content Area

The content area displays transactional information related to the infotile you select. You can review the detailed information and take the necessary action.

For example, click the item link in the table to drill down to transaction-level information. You can perform multiple actions on the transaction, such as editing the invoice, approving or rejecting the transaction, and posting the invoice to the ledger.

Actions Toolbar

Use the actions toolbar to perform a range of activities on one or more rows you select in the content area.

For example, select a transaction row and use the View menu to view the transaction in more detail. You can export the data to an Excel worksheet, detach the pane, approve or reject one or more transactions, as well as apply additional filters.

Tasks Panel Tab

The Tasks pane includes tasks that are related to the work area and that you have access to perform.

For example, create an invoice, review journal entries, create mass additions, and manage accounting periods within a task pane.

Search Panel Tab

Search enables you to find a specific transaction using search criteria related to the work area.

For example, search on an invoice number or supplier in the Invoices work area to find a specific transaction.

Reports and Analytics Panel Tab

The Reports and Analytics panel tab contains predefined reports as well as a folder for you to set up your own reports.

For example, use the predefined reports to perform a deeper analysis on invoices above a certain dollar amount without a PO. You can also access reports that you have copied and modified and stored in your own folder.

Overview of Your System Integrator

After you determine the applications to implement, complete any steps that are needed for your implementation plan in Oracle Global Human Resources first to address any dependencies with Oracle Financials.

Your system integrator uses his or her implementation expertise to help you with a smooth transition to Oracle Financials. They also use the Rapid Implementation task list to help you achieve a successful implementation in the shortest time possible.

Related Topics

Purchase and Activation of Oracle Fusion Cloud Applications

Purchase, activate, and manage services for Oracle Fusion Cloud Applications services.

The process involves:

- Purchasing and activating your services.
- Verifying that the services are activated, monitoring the services, and performing other administrative tasks.

Service Purchase and Activation

Your buyer or an Oracle sales representative orders a cloud service and specifies information about the account administrator during the ordering process. The account administrator performs the functions of both the service administrator and the tenancy administrator.

Here's how your buyer can order a subscription:

1. Go to *Oracle Cloud Applications* to browse applications and compare products and features.
2. When ready to order, click **Contact Sales** to chat, call, or submit a message to Oracle Sales.

The account administrator receives an email to activate the service. As part of activation, the account administrator associates the new cloud subscription with an Oracle account.

See: *Activating Your Oracle Cloud Applications Order*

Service Availability in US Government Regions

If you're in noncommercial regions within the US, contact your Oracle account or sales representative for details about service and feature availability in your regions.

Alternative Versions of Specified Oracle Services

From time to time, at Oracle's sole discretion, Oracle may make alternative versions of specified Oracle services available for customers to access on a limited basis. These alternative versions may not have the same feature sets as the versions of these services for which a fee is paid, and Oracle may terminate and no longer make available these alternative versions at any time.

Next Steps

- The administrator who's identified during the activation process creates backup tenancy administrators for managing and monitoring the service.

  See: *Managing Oracle Cloud Users with Specific Job Functions*

- The same administrator or any of the tenancy administrators would manage and monitor the service, including creating and managing environment families and environments.

  See: *Fusion Applications Environment Management*

  - As part of managing an environment, the administrator adds Fusion administrators.

    See: *Environment Management Tasks*
  - Fusion administrators can sign in to Fusion Applications and get other users set up so that they can also sign in and work in Fusion Applications.
- Functional implementors perform configuration and setup steps in Fusion Applications.
- Developers can add features to extend the application.
- Your cloud service will be updated regularly.

  See: *Oracle Applications Cloud - Fusion Applications Update Policy (KB160632)* on *My Oracle Cloud Support*.

2 Oracle Cloud Security

Overview of Implementing Financials Security

Oracle Financials provides common job roles such as Accounts Payable Manager and General Accounting Manager. You can use these roles, modify them, or create job roles as needed.

> **Note:** Since you can assign multiple roles to a user, don't define a role that includes all the accesses needed for every user.

To review the predefined job roles in Oracle Financials, see the Oracle Fusion Cloud Financials Security Reference guides in the Oracle Help Center (http://docs.oracle.com).

To find more information on securing your applications, see the Oracle Fusion Cloud ERP Securing ERP guide in the Oracle Help Center (http://docs.oracle.com).

Related Topics

Other Financials Security Considerations

Common functionality that's not job specific, such as creating expense reports and time cards, are granted to the abstract role **Enterprise Resource Planning Self Service User**. Abstract roles like **Employee**, **Contingent Worker**, and **Line Manager** also grant access to common functionalities across a wide collection of Oracle Fusion Cloud Applications.

A library of duty roles, packaging access to respective Transaction Business Intelligence subject areas and corresponding detail pages, are also available as building blocks to provide self-service reporting access.

Oracle Fusion Cloud Financials includes the following roles that are designed for initial implementation and the ongoing management of setup and reference data:

- **Application Implementation Manager:** Used to manage implementation projects and assign implementation tasks.
- **Application Implementation Consultant:** Used to access all setup tasks.
- **IT Security Manager:** Used to access the Security Console to manage roles, users, and security.
- **Financial Integration Specialist:** Used to plan, coordinate, and supervise all activities related to the integration of financials information systems.

> **Note:** For the ongoing management of setup and reference data, the predefined **Financial Application Administrator** role provides access to all financial setup tasks.

Separation of Duties Considerations

Separation of duties (SOD) separates activities such as approving, recording, processing, and reconciling results so you can more easily prevent or detect unintentional errors and willful fraud.

Oracle Financials includes prebuilt roles that can accelerate deployment. To find out whether they could be valuable to your organization:

1. Gather your FIN stakeholders, for example, the owners of business processes, IT security administrators, and internal audit / financial governance teams.
2. Identify the prebuilt roles that are relevant to your FIN activities.
3. Determine whether those roles should be used as is, or fine-tuned to suit your operational, security, and compliance requirements. For example, if a user has the Create Payments and Approve Invoice privileges, you might consider it an SoD conflict. The predefined Accounts Payable Manager role has the privileges of Force Approve Invoices and Create Payments. When you assess and balance the cost of duty separation against reduction of risk, you might determine that the Accounts Payable Manager role should not be allowed to perform Force Approve Invoices and remove that privilege.

To learn more about SoD, see Using Advanced Controls in the Oracle Help Center (http://docs.oracle.com). To learn more about the policies and roles, see the Security Reference Manuals in the Oracle Help Center.

Data Security Considerations

- Use segment value security rules to restrict access to transactions, journal entries, and balances based on certain values in the chart of accounts, such as specific companies and cost center values, to individual roles.
- Use data access set security for Oracle General Ledger users to control read or write access to entire ledgers or portions of the ledger represented as primary balancing segment values, such as specific legal entities or companies.

For more information on securing your applications, see the Oracle Fusion Cloud ERP Securing ERP guide in the Oracle Help Center (http://docs.oracle.com).

Related Topics

Security for Country-Specific Features

For new implementations, you must assign the country-specific duty roles to your enterprise job roles or users to use the features specific to these regions.

You must assign custom roles based on the following country-specific duty roles to FSCM application and OBI application stripe. After assigning these custom roles you can view the country-specific reports on the Scheduled Processes page, and open the Parameters page of the selected process.

This table describes the duty roles for each region:

Region	Duty Role	Role Code
Europe, the Middle East, and Africa (EMEA)	EMEA Financial Reporting	ORA_JE_EMEA_FINANCIAL_REPORTING_DUTY
Asia Pacific (APAC)	APAC Financial Reporting	ORA_JA_APAC_FINANCIAL_REPORTING_DUTY
Asia Pacific (APAC)	Enterprise Financial Data Export Management for China	ORA_JA_CN_ENTERPRISE_FINANCIAL_DATA_EXPORT_ONLY_FOR_CHINA_DUTY_OBI

Region	Duty Role	Role Code
Asia Pacific (APAC)	Golden Tax Management for China	ORA_JA_GOLDEN_TAX_MANAGEMENT_FOR_CHINA_DUTY_OBI

General Ledger

Overview of General Ledger Security

General ledger functions and data are secured through job roles, data access sets, and segment value security rules.

Functional Security

Functional security, which is what you can do, is managed using job roles. The following job roles are predefined for Oracle General Ledger:

- General Accounting Manager
- General Accountant
- Financial Analyst

Each job role includes direct privilege grants, as well as duty role assignments, to provide access to application functions that correspond to their responsibilities. For example, the General Accounting Manager role grants comprehensive access to all General Ledger functions to the general accounting manager, controller, and chief financial officer in your organization.

Data Security

Data security, which controls what action can be taken against which data, is managed using:

- Data access sets
- Segment value security rules

Data access sets can be defined to grant access to a ledger, ledger set, or specific primary balancing segment values associated with a ledger. You decide whether each data access set provides read-only access or read and write access to the ledger, ledger set, or specific primary balancing segment values, which typically represent your legal entities that belong to that ledger. Primary balancing segment values without a specific legal entity association can also be directly assigned to the ledger.

Segment value security rules control access to data that's tagged with the value set values associated with any segment in your chart of accounts.

Security Assignment

Use the Security Console to assign users roles (job roles, as well as roles created for segment value security rules or others). Use the Manage Data Access Set Data Access for Users task to assign users data access sets as the security context paired with their General Ledger job role assignments.

For more information about security assignments and managing data access for users, see the Oracle ERP Cloud Securing ERP guide.

Related Topics

- Data Access

Overview of Data Access Set Security

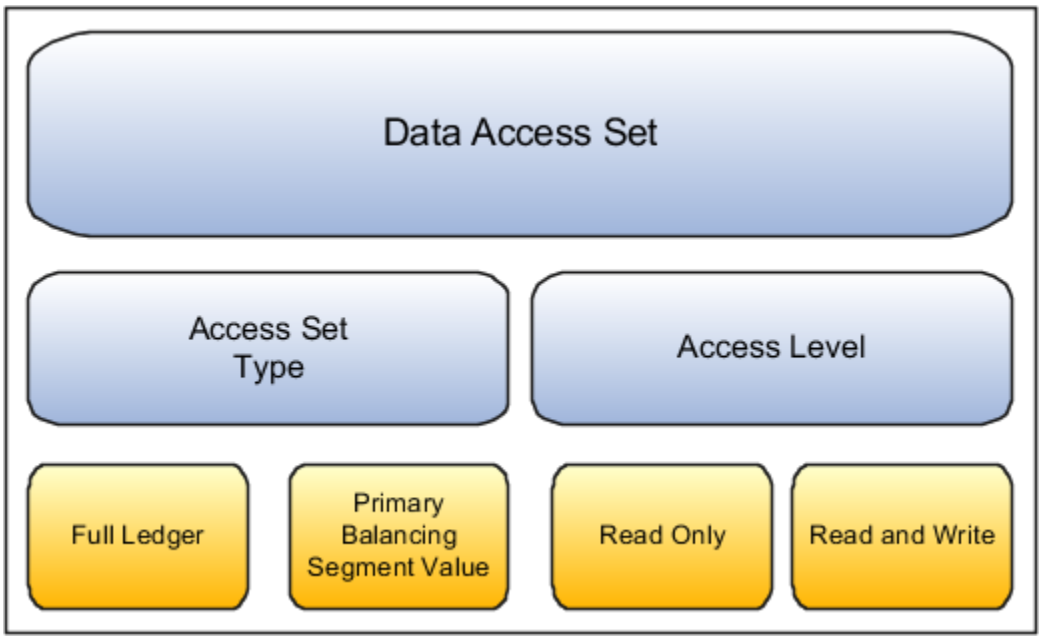
Data Access Sets secure access to ledgers, ledger sets, and portions of ledgers using primary balancing segment values.

If you have primary balancing segment values assigned to a legal entity, then you can use this feature to secure access to specific legal entities.

You can combine ledger and ledger set assignments in single data access sets if the ledgers share a common chart of accounts and calendar. If you have primary balancing segment values assigned to a legal entity within the ledger, then you can use data access sets to secure access to specific legal entities. You can also secure access to primary balancing segments assigned directly to the ledger.

When a ledger or ledger set is created, a data access set for that ledger or ledger set is automatically created, giving full read and write access to those ledgers. You can also manually create data access sets to give read and write access, or read-only access to entire ledgers or portions of the ledger represented as primary balancing segment values.

The following figure shows that a data access set consists of an access set type and an access level. The access set type can be set to full ledger or primary balancing segment value. The access level can be read only or read and write.



The **Full Ledger** access set type provides access to the entire ledger or ledger set. This could be for read-only access or both read and write access to the entire ledger.

The **Primary Balancing Segment Value** access set type provides access to one or more primary balancing segment values for that ledger. This access set type security can be specified by parent or detail primary balancing segment values. The parent value must be selected from the tree that's associated with the primary balancing segment of your chart of accounts. The specified parent value and all its descendants, including middle level parents and detail values

are secured. You can specify read only, read and write access, or combination of both, for different primary balancing segment values for different ledgers and ledger sets.

For more information about security assignments and managing data access for users, see the Oracle ERP Cloud Securing ERP guide.

Examples of Data Access Set Security

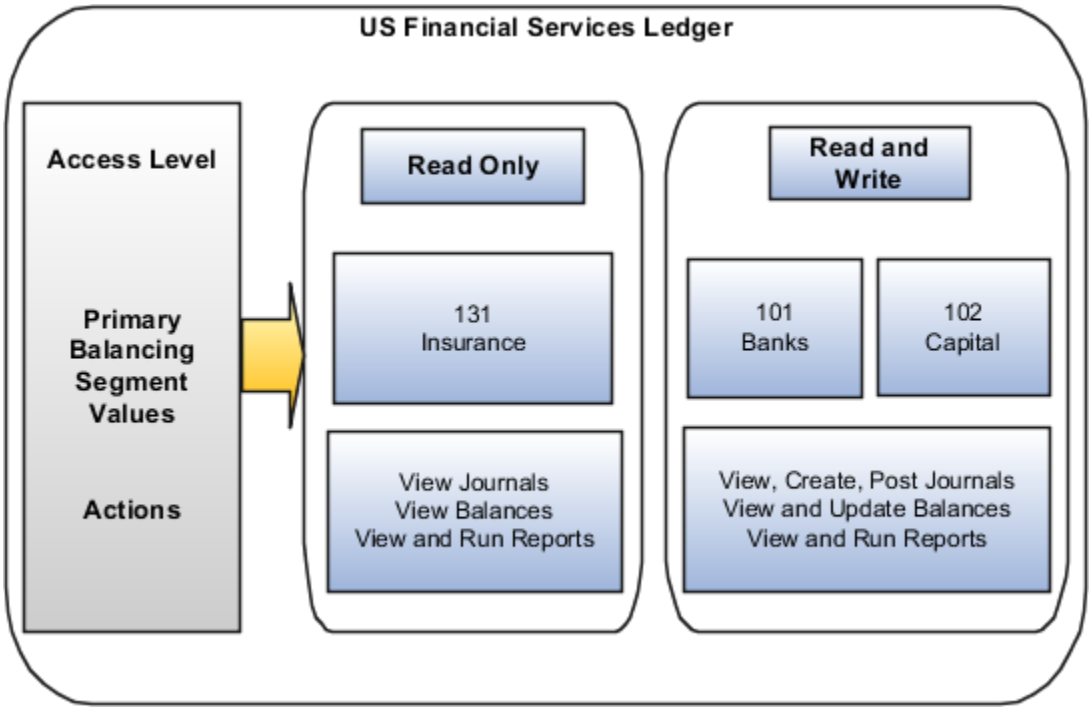
This example shows a data access set that secures access by using primary balancing segment values that correspond to legal entities.

Scenario

The following figure shows a data access set for the US Financial Services Ledger. The access set type is Primary Balancing Segment Value, with each primary balancing segment value representing different legal entities. Read-only access has been assigned to primary balancing segment value 131, which represents the Insurance legal entity. Read and write access has been assigned to primary balancing segment values 101 and 102, which represent the Banks and Capital legal entities.

For this data access set, the user can:

- View the journals, balances, and reports for primary balancing segment value 131 for the Insurance legal entity.
- Create journals and update balances, as well as view journals, balances and reports for primary balancing segment value 101 and 102 for legal entities Banks and Capital.



Note: In financial reporting, the list of ledgers isn't secured by data access sets when viewing a report in Preview mode. Users can view the names of ledgers they don't have privileges to view. However, the data from a secured ledger doesn't appear on the report.

For more information about security assignments and managing data access for users, see the Oracle ERP Cloud Securing ERP guide.

Overview of Segment Value Security

Segment value security provides chart of accounts security to secure access to create or view financial data.

Selectively enable enforcement using segment value security rules by business function, including by General Ledger, Payables, Receivables, Assets, Intercompany and Subledger Accounting. Security administrators can grant account values access to users based on certain business functions, data security context, and read-only or read and write access levels. For all other product modules, there is no enforcement when security is enabled for the chart of accounts segment value set, and users working with these other modules will have access to all accounts.

Here are some business benefits that chart of accounts segment values security provides.

- Provides precision in securing account access for each user to each product module, including General Ledger, Payables, Receivables, Assets, Intercompany and Subledger Accounting. Limit security enforcement to the modules where this is required.

  This feature addresses a wide range of financial data security requirements by providing a chart of accounts-based data security control using highly precise grants of secured account values to users qualified by:
  - Business function
  - Data security context
  - Read only versus read and write access level

  A user's access to specific account values can be selectively provided with rule assignments that are tagged with a business function and data access context such that the grant would only apply for that user under the matching usage scenario. Moreover, the access can be granted on a read and write or read-only basis. If there are no matching rule assignments for that user for a given usage scenario, the user gets access to all account values for the secured chart of accounts value set.

  This ensures that all users only get the exact and appropriate access to the financial data they need to work with.

  For example, with the General Ledger business function you might have some select accountants in your organization who not only manage the financial accounting for their region but are also responsible for calculating the global bad debt reserve. They require full read and write access to all accounts when working with the financial data specific to their assigned region but should have read-only access to specific accounts of the worldwide financial data related to calculating the global bad debt reserve. It would be possible to achieve this type of access control with this feature by enabling security enforcement for the General Ledger business function. Such users would then be assigned rules that granted read-only access to those select bad debt reserve related accounts when working with the global ledgers outside of their region, while being given access to all accounts on a read and write basis when working with their regional ledger.
- Reduce the time needed to set up and maintain rules. Users with unrestricted access to accounts are automatically granted all account values; users who require restricted access are assigned an explicit security configuration.

  Streamlined configuration and administration of this chart of accounts security feature is achieved by selectively enabling security enforcement for distinct business functions. Simplified onboarding via management by exception is achieved through initially providing access to all secured account values by

default to all users. Only those users who should work with just certain accounts for their given usage scenarios need to be actively managed and assigned distinct rules to limit their access.

Setup efficiency is optimized with rule assignments that can be flexibly configured with varying degrees of specificity to fit the unique data security requirements of a particular user. Generic rule assignments can be shared between groups of users with similar access requirements to secured accounts.

Key Steps for Configuring Chart of Accounts Segment Value Security

Here are the main steps for setting up chart of accounts segment value security.

1. Select business functions that enforce segment value security.
2. Enable security for a value set.
3. Deploy the accounting flexfield and publish account hierarchies.
4. Prepare the Manage Segment Value Security Rules spreadsheet.

Before you start, you'll need to have a role that's based on either the Application Implementation Consultant (ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB) or the Financial Application Administrator (ORA_FUN_FINANCIAL_APPLICATION_ADMINISTRATOR_JOB), and the IT Security Administrator (ORA_FND_IT_SECURITY_MANAGER_JOB) job roles to have access to the range of functions required to set up all the elements involved with configuring segment value security by business function for users in the application.

The Manage Advanced Chart of Accounts Segment Value Security (FUN_MANAGE_ADVANCED_CHART_OF_ACCOUNTS_SEGMENT_VALUE_SECURITY_PRIV) privilege controls access to the Manage Segment Value Security Rules spreadsheet. You'll need a custom role that's assigned this privilege.

Select Business Functions That Enforce Segment Value Security

The business functions that you select affect all secured value sets in all charts of accounts that the value sets are used in.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
    - Offering: Financials
    - Functional Area: Financial Reporting Structures
    - Task: Manage Chart of Accounts Configurations

2. Click **Manage Segment Value Security by Business Function**.

> **Note:** If the button doesn't appear, your instance doesn't qualify for segment value security by business function. Only instances with no secured value sets at the time they're evaluated will be qualified to use this model of chart of accounts segment value security. For an instance where there's at least one existing value set enabled for security, including one that's assigned to your chart of accounts segment or other application key flexfields, it will continue to behave in the same manner as it had all along in previous releases, enforcing segment value security without the business function distinction. Any future value set enabled for security in such an instance will also apply enforcement in this same manner. For more information, see the *Segment Value Security without Business Function Implementation Guide* (Doc ID 3054824.1) on My Oracle Support.

> **CAUTION:** The evaluation and designation for a Cloud Applications environment of the enforcement method of segment value security by business function or without business function is applied distinctly on each instance, based on their distinct instance name plus instance type. Two instances with the same letter name but of different types (that is, instance WXYZ Prod versus instance WXYZ Test) are considered individually, and the segment value security enforcement method will be set for each instance based on the presence or absence of value sets enabled for security, independent of the other like-named instance.

3. On the Manage Segment Value Security by Business Function dialog box, review this text, which appears after the title.

   You're enabling segment value security for your chart of accounts for the very first time. Select the business functions where segment value security must be enforced. Your selections will apply to all charts of accounts whose segments are enabled for security. Click **Cancel** to make your selection later.
4. Select the business functions where security must be enforced.

> **Note:** A business function can be disabled from security enforcement afterward.

   You can select from among the following business functions:
   - General Ledger
   - Payables
   - Receivables
   - Intercompany
   - Assets

   Selecting one or more of these business functions automatically enables security enforcement for Oracle Subledger Accounting because it's an integration module between Oracle General Ledger and the other listed subledger business functions.

> **Note:** You don't have to make all your business function selections at once. You can select additional business functions later by clicking Manage Segment Value Security by Business Function.

Enable Security for a Value Set

After selecting the business functions, the next step is to enable security for a chart of accounts value set for the Accounting Flexfield (GL#) key flexfield.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
    - Offering: Financials
    - Functional Area: Financial Reporting Structures
    - Task: Manage Chart of Accounts Configurations

    > **CAUTION:** You must use this task and the Manage Chart of Accounts Configurations page to enable security for a value set. Don't use the Manage Value Set, Edit Value Set, or Edit Value Set Data Security pages because the required initialization for the value set won't be successful and the security configuration for the value set won't be correct.

2. Click the name of the chart of accounts that you want to secure.
3. In the Segments section, select the segment row with the value set that you want to secure.

    Value set security applies at the value set level, not to individual segments of a chart of accounts that reference that value set. If a value set is used in multiple charts of accounts, then all chart of accounts segments that are assigned that value set will be enabled for security.

    Chart of accounts security is enabled for one value set at a time, and its security rules and rule assignments are framed individually for each distinct secured value set for which they're defined.

    For a chart of accounts that has multiple segments with secured value sets, each value set's security configurations are considered individually and they're not cross-secured with one another. To determine whether an account combination that a user is working with passes the access check for each of account combination segments' values, the grants for the individual secured segments are each evaluated independently and then applied additively across each of the secured segments.

    > **CAUTION:** For a secured Accounting Flexfield (GL#) value set that's shared with other key flexfields, such as the Budgeting Flexfield (XCC), the Cost Allocation Flexfield (COST), the Asset Key Flexfield (KEY#), the Location Flexfield (LOC#), and others, security will not be enforced for that secured value set with these other types of key flexfields. Value sets in other types of key flexfields that aren't shared with the Accounting Flexfield (GL#) key flexfield and that are enabled for security will still enforce segment value security in the mode without the business function distinction. As such, there can be differences in segment value security enforcement across the segments of such key flexfields.

4. On the Value Set tab in the Value Set section, select **Enable security.**

    > **Note:** If you're enabling security on a value set for the first time and you haven't performed the previous setup step of selecting the business functions that enforce segment value security, the Manage Segment Value Security by Business Function dialog box will open. See the *Select Business Functions That Enforce Segment Value Security* topic for more information.

    It's possible to deselect the **Enable security** checkbox and stop enforcement of segment value security for a value set. If you deselect the checkbox, you must redeploy the GL# Accounting Key Flexfield to process such a metadata change to the chart of accounts for this to take effect. Successful redeployment is similarly required when enabling or disabling security for a value set referenced in any other type of key flexfield, such as the Budgeting Flexfield (XCC).
5. Click **Save**.

The application will automatically create the data security resource for the secured value set. The security object name uses the format **DS** followed by an underscore (_) and then the value set name, without spaces. For example, if the value set name is **Vision Company**, then the data resource security name would be **DS_VisionCompany**.

In addition, the application generates an **All Values** policy for this data security resource to the Authenticated User (ORA_FND_AUTHENTICATED_USER_ABSTRACT) role, which is automatically assigned to all users who successfully sign in to the application. The policy name follows this format: **<Secured Value Set Name> – All Segment Values**, for example, **Vision Company – All Segment Values**. This policy is the key mechanism enabling the segment value security by business function behavior where all users are first provided access to all account values of a secured value set by default. This default policy will be suppressed in usage scenarios where a user has a matching distinct policy assignment that restricts access to certain account values.

Deploy the Accounting Flexfield and Publish Account Hierarchies

When enabling or disabling security for a chart of accounts value set, you must successfully deploy the accounting flexfield for the change to take effect.

In the Setup and Maintenance work area, use the Manage Chart of Accounts Configurations task in the Financial Reporting Structures functional area and click **Deploy All Charts of Accounts**.

> **Note:** You can monitor the progress of the Accounting Flexfield deployment using the Manage Chart of Accounts Structures task.

To update the General Ledger balances cube so that the current security enforcement settings are applied, you must publish the account hierarchies for the secured value sets. In the Setup and Maintenance work area, use the **Publish Account Hierarchies** task in the Financial Reporting Structures functional area.

Related Topics

- When does security take effect on chart of accounts value sets for balances cubes?
- What happens when changes are made to an account hierarchy that's referenced in segment value security rules?

Open the Manage Segment Value Security Rules Spreadsheet

If there are users who should have access to only limited accounts of a secured value set at all times, or for their certain usage scenarios, then you must configure rules and user rule assignments for that secured value set.

This is necessary to suppress the All Values access that was granted by default to every user, which is a feature of segment value security rules by business function.

You must use the Manage Segment Value Security spreadsheet exclusively to maintain your rules and rule assignments for segment value security by business function.

Don't use the following methods to create or maintain rule and rule assignment setups for secured value sets:

- Edit Data Security page in the application.
- Rapid Implementation Create Segment Value Security Rules spreadsheet, which is opened using the Create Segment Value Security Rules in Spreadsheet task.

The Manage Segment Value Security Rules spreadsheet captures additional rule and rule assignment attributes that aren't maintained in the Edit Data Security page or in the Rapid Implementation Create Segment Value Security Rules spreadsheet, including attributes that support enforcing segment value security by business function.

Commingling the usage of the Manage Segment Value Security Rules spreadsheet with the Edit Data Security page or the Rapid Implementation spreadsheet to maintain your segment value security setups will result in serious data inconsistencies that will cause the incorrect enforcement of segment value security.

After you've saved your changes to enable security for a value set, you can open the Manage Segment Value Security Rules spreadsheet to set up your security rules.

1. In the Setup and Maintenance work area, go to the Manage Chart of Accounts Configurations task:
    - Offering: Financials
    - Functional Area: Financial Reporting Structures
    - Task: Manage Chart of Accounts Configurations
2. On the Manage Chart of Accounts Configurations page, select the chart of accounts.
3. In the Segments section, select the secured value set.
4. In the Value Set tab, click **Manage Data Security**. The spreadsheet will open within the context of the secured value set.

Related Topics

- Set Up Desktop Integration for Excel
- Guidelines for Using Desktop Integrated Excel Workbooks
- Troubleshoot Desktop Integration for Excel

Using the Manage Segment Value Security Rules Spreadsheet

Follow these guidelines when creating new rules and new rule assignment records in the Manage Segment Value Security Rules Spreadsheet.

- Always navigate to the Rules sheet first to initialize your session, then second to the Rule Assignments sheet. Don't navigate directly to the Rule Assignments sheet right away because this will result in an error for your session with the spreadsheet.
- Click the Upload command on the Manage Segment Value Security tab once you've completed your entries on the worksheet to save these records to the application.
- Upload the Rules worksheet first before completing and uploading the Rule Assignments worksheet because the assignments in the latter worksheet reference the rules. The rules need to be successfully saved to the application first before they can be assigned to users.
- Work with only one secured value set at a time per session. Otherwise, the application can't properly identify which value set is the focus if multiple secured value sets are simultaneously being worked on. As part of its initialization, the spreadsheet establishes a connection and value set of focus.

Create Rules

The Rules worksheet of the Manage Segment Value Security Rules spreadsheet is for defining segment value security policies.

Policies can include one or more segment value security condition filters and are associated with a segment value security role. The segment value security role serves as the conduit to pass the security policy to users.

A policy can have a one-to-many relationship with condition filters. You can do this in the spreadsheet by using the same policy name across multiple rows. The different condition filters defined in these multiple rows will be treated as a group that's associated with that one policy. This helps you adhere to the best practice of keeping in check the number of security policies defined for a secured value set and keeping setups manageable.

Columns are either policy-level attributes or condition filter-level attributes. Policy-level attributes must share the same value across multiple rows for the group of condition filters that are part of that same policy. Values for the condition filter-level attributes representing the different condition filters that you want to apply to the same policy will vary across the rows.

Enter attribute values in the order in which the columns appear in the worksheet, starting with the policy name.

This table lists the attribute columns on the Rules worksheet and their properties.

Attribute	Required	Updatable	Policy or Condition Filter Attribute
Policy Name	Yes	No	Policy
Policy Description	No	Yes	Policy
Segment Value Security Role Name	Yes	No	Policy
Operator	Yes	Yes	Condition Filter
From Value (Used with all operators other than All Values)	Yes	Yes	Condition Filter
To Value (Used with Between operator only)	Yes	Yes	Condition Filter
Tree Code (Used with hierarchical operators only)	Yes	Yes	Condition Filter
Tree Version (Used with hierarchical operators only)	Yes	Yes	Condition Filter
Policy Start Date	Yes	No	Policy
Policy End Date	No	Yes, if the policy is active, that is, the policy end date is today's date or later.	Policy
Mark for Deletion	No	Yes	Condition Filter

Here's more information about each attribute to help you prepare the Rules worksheet.

Policy Name

Identifies the specific condition to segment value security role association. The name must be unique within the individual secured value set. The application automatically stores the capitalized policy name to help minimize confusion and anomalies when referencing the policy's name.

Policy Description

Provides a summary of the scope, purpose, or other pertinent information about the policy.

Segment Value Security Role Name

Identifies the predefined role to which you're assigning the segment value security policy. Double-click within the cell to open a dialog box, where you can select the role to insert into that cell. To form a complete user rule assignment, you must also assign the segment value security role of the policy to the users you want to assign the policy.

Operator

Indicates how to evaluate the succeeding values specified in the row for the purpose of determining what account values of the secured value set are being granted. This is a key attribute of a segment value security condition filter.

Related condition rows for the same policy created using the spreadsheet will always be set to the Match Any option or to using the Or conjunction when stringing together the various condition filter rows for the same policy to determine what account values are involved. This is also the default match setting even if it's a policy with just a single condition filter row.

This means that the account values being granted by the policy just need to match one of the condition rows stipulated in the group, rather than simultaneously match every one of the condition rows in that group, which would more than likely result in a nonmatch, or no account value, because an account value is unlikely to satisfy every one of those conditions.

This table describes the operators you can use in the condition filters.

Operator	Description
All Values	Provides access to all account values in the value set.
Equal to	Provides access to a specific account value. When the specified value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. The rule doesn't provide access to any of its descendants.
Not equal to	Provides access to all values, except the one detail/child or a parent value that you specify. In the case of a parent value, the exclusion only applies specifically to that parent value itself, and not any of its descendant parent and detail or child values.

Operator	Description
	CAUTION: Here are some important points about this operator. • Use this operator carefully and sparingly. • Don't use it in multiple condition rows for the same policy or in different policies assigned to the same security value security role for a given secured value set. The different conditions could end up canceling each other out, resulting in unintended access being granted to account values you want to secure. For example, let's say you have a policy with two condition rows. You define the first condition as Not Equal To account value 100 and the second condition as Not Equal To account value 200. The list of values for the segment is going to show both 100 and 200, among other values. That's because an account value can meet any one of the conditions for the rule to apply. The value of 100 meets the Not Equal To 200 condition and the value of 200 meets the Not Equal To 100 condition.
Between	Provides access to the account values included in the range of values specified in the From and To Value columns. When the range of values includes a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. The rule doesn't provide access to any of its descendants, unless they're part of the specified range.
Contains	Provides access to account values that contain the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless those descendants also happen to match the condition.
Ends with	Provides access to account values that end with the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless those descendants also happen to match the condition.
Starts with	Provides access to account values that start with the specified value. When the matching value is a parent account, access applies to that parent value only, in all trees and tree versions that include that parent. It doesn't provide access to any of its descendants unless the descendants also happen to match the condition.
Is descendant of	Provides access to the specified parent account value and all its descendants. Descendants include middle level parent accounts and nonparent accounts throughout all that parent's hierarchical branches, from the root to the leaf nodes.
Is last descendant of	Provides access to the specified parent account value and to the account values at the leaf nodes of that parent. Access doesn't include intermediate parent account values along the hierarchical branches.

Note: For the **Is descendant of** and **Is last descendant of** operators, the security rule provides access across all tree versions of the specified hierarchy that reference the accounts that are granted, as well as all hierarchies associated with the same value set of the specified hierarchy. It uses the parent value rollup of the rule's specified hierarchy as the basis for determining which values are granted and applies date effectivity to identify which is the effective version based on the system date for the rule's specified hierarchy and the account values included in that version. For more information see the *Reporting on General Ledger Balances Cubes Reports with Account Hierarchies* topic.

From Value

Specifies the value to apply for the specified condition filter operator in determining what account values to consider. You must specify a valid account value when using any condition filter operator, except for Between, Contains, Ends with, and Starts with. This allows for some additional flexibility to include account values that have yet to be created.

To Value

Specifies the value to apply for the Between condition filter operator in determining what account values to consider. This is the ending value for the range and allows for some additional flexibility to include account values that have yet to be created.

Tree Code

Identifies the tree to reference when you select a parent account value for the condition. This is a required attribute if you're using the **Is descendant of** and **Is last descendant of** operators. These operators are also the only valid operator choices when you specify a tree code for the row. Double-click within the cell to open a dialog box, where you can select a valid tree code for the secured value set that you're working with.

While a distinct tree code is associated with each segment in a chart of accounts, as specified by the Default Hierarchy value in the chart of accounts structure setup, you can refer to any tree that's defined for the secured value set.

> **Note:** The trees that you specify in a rule must be flattened. This contrasts with trees that are published to balances cubes, which don't need to be flattened. If your security rules refer to trees that are published to the balances cubes, then the trees must be flattened. Otherwise security enforcement won't work in balances cube-based reports and queries.

Tree Version

Identifies the tree version of the selected tree code to reference when you select a parent account value for the condition. This is a required attribute if you're using the **Is descendant of** and **Is last descendant of** operators. These operators are also the only valid operator choices when you specify a tree version for the row.

Policy Start Date

Specifies when the policy begins. You must specify a start date that's no earlier than the current system date when creating the policy because a policy can't be effective for any earlier date than when it comes into existence. You can also specify a future date.

This attribute must share the same value among related rows of multiple condition filters that are tied to the same policy.

> **Note:** When you add new condition filter rows to an existing policy, the start date for the new rows must match the start date of the original policy rows because this is a policy-level attribute.

Policy End Date

Specifies when the policy ends. You must specify an end date that's no earlier than the policy start date. If you don't specify an end date, then the policy is in effect indefinitely.

You can update the end date on an existing policy as long as the specified end date is today or a date in the future. That is, the rule is still active. The new end date must be at least today's date or a date in the future. There's no requirement for the new end date to be later than the current end date.

For example, let's say today's date is January 27 and the end date for a rule is set to January 31. A day later, on January 28, you can update the end date to January 28 or later. It doesn't have to be set beyond January 31, which is the original end date. However, you can't update the end date from January 31 once it's February 1.

This attribute must share the same value among related rows of multiple condition filters that are tied to the same policy.

> **Note:** When you add new condition filter rows to an existing policy, the end date for the new rows must match the end date of the original policy rows, if there is one, because this is a policy level attribute.

For audit purposes, segment value security policies are never deleted. The Policy End Date attribute is used instead to indicate that the policy is no longer applicable.

Mark for Deletion

Indicates whether to delete the selected condition filter row and remove it from the policy. This deletion indicator safeguards users from accidentally deleting condition filter rows for a policy from the application by requiring users to explicitly indicate this action for a given row. This is a condition-level attribute and individual condition filter rows associated with the policy can be specifically marked for deletion.

> **Note:** If the only condition filter row for a given condition is marked for deletion, the application will automatically end date the policy and no longer display such empty policies in the spreadsheet, that is, a policy with no condition filter rows.

Related Topics

- Using the Manage Segment Value Security Rules Spreadsheet

Create Rule Assignments

The Rule Assignments worksheet of the Manage Segment Value Security Rules spreadsheet is for assigning policies to users, qualifying under which business function and security context the policy assignments are applicable for the user, and granting either a read only, or a read and write access level.

Enter attribute values in the order in which the columns appear in the worksheet.

This table lists the attribute columns on the Rule Assignments worksheet and their properties.

Attribute	Required	Updatable
User Name	Yes	No
Policy Name	Yes	Yes
Role Name (Display Only)	Not applicable	Not applicable
Business Function	Yes	Yes
Security Context	Yes	Yes
Security Context Value	Yes	Yes

Attribute	Required	Updatable
Access Level	Yes	Yes
Start Date	Yes	No
End Date	No	Yes

Here's more information about each attribute to help you prepare the Rule Assignments worksheet.

User Name

Identifies the user for the rule assignment. Select one of the following options:

- **Select specific**: Select to specify the sign in name of the user who's to be assigned the rule or policy for the given secured value set.
- **Select all assigned to the policy role**: Select to share the rule assignment with all users who are assigned the role for the specified policy.

Policy Name

Identifies the policy to assign to the user. Double-click within the cell to open a dialog box, where you can select a valid policy for the given secured value set.

Role Name

Identifies the role associated with the policy selected for the rule assignment. This is a display-only field and is shown as additional information when searching and retrieving a rule assignment from the application.

Business Function

Identifies the business function that the rule assignment for the user applies to. The list corresponds to the product modules that support segment value security by business function.

> **Note:** To create a rule assignment for a given business function, that function must be enabled for segment value security enforcement.

This table lists the business functions and their corresponding product modules.

Business Function	Product Module
Assets	Oracle Assets
General Ledger	Oracle General Ledger
Payables	Oracle Payables
Provider intercompany	Oracle Intercompany
Receivables	Oracle Receivables
Receiver intercompany	Oracle Intercompany

Selecting any of these business functions automatically includes Oracle Subledger Accounting, a product module that integrates between General Ledger and the subledgers.

> **Note:** The 2 Intercompany business functions allow you to further differentiate whether the rule assignment to the user for the specified intercompany organization is applicable when the intercompany organization is being used by the user to transact in the capacity of a provider or a receiver.

You can also select **All business functions** if the grant of the policy to the user isn't limited for just a particular business function. It can also be used in the case of the Intercompany module when the rule assignment to an Intercompany user applies no matter when the specified intercompany organization is transacting in the capacity of a provider or receiver.

The selection for this attribute also determines which choice is valid for the following **Security Context** attribute because the security context corresponds to the selected business function.

Security Context

Identifies the type of security context under which the policy or rule assignment should be valid for the user. You must select a security context that correlates to the selected business function. For example, for the General Ledger business function, the applicable security context is data access set.

Here are the possible choices:

- Business unit: Applies to the Payables and Receivables business functions.
- Asset books: Applies to the Assets business function.
- Data access set: Applies to the General Ledger business function.
- Intercompany organization: Applies to the Intercompany business functions.
- All security contexts: Applies to any business function.

> **Note:** If you want to include the business unit for both the Payables and Receivables business functions, select **All business functions** for the Business Function attribute.

The selection for this attribute also determines which choice is applicable for the following **Security Context Value** attribute because the context value corresponds to the selected security context.

If it isn't necessary to limit a user's policy to be applicable for a particular security context and security context value, you can select **All security contexts**. This selection can be paired with the selection of **All business functions**, or a specific business function, in the preceding column. For the former, this means that the rule assignment or policy grant for the user will be applicable no matter what business function, security context, and security context value that user is working with. It effectively means that this policy is applicable for the user all the time. If a specific business function is selected, the rule assignment is applicable to the user only for the selected business function, but without regards to the security context value that user is working with.

If you select **All security contexts**, the only valid choice for the **Security Context Value** attribute is **All security context values**.

Security Context Value

Specifies the security context value for the selected security context type and business functions in the preceding 2 columns under which the policy or rule assignment will be effective for the user. The possible choices include the valid asset books, business units, data access sets, or intercompany organizations in the system, depending on the security context that was selected for the rule assignment.

For the policy or rule assignment to be a relevant and effective one for the users to which they're assigned, ensure that the selected asset book, business unit, data access set, or intercompany organization for that rule assignment is one that's assigned to the user in the Manage Data Access for Users page and to which the user has been granted data access.

There's also a choice of **All security context values**, which is the only valid choice when **All security contexts** is selected for the preceding **Security Context** column. This would make this policy always applicable to the user, no matter what data access context that user is working with.

Access Level

Indicates whether the user rule or policy assignment for the given business function, security context, and context value should be granted on a **Read only** or **Read and write** basis.

For rule assignments that are set to **Read only**, the account values allowed will only be applicable in read-only features, such as an inquiry page or a report. Where the product feature involves update capabilities for accounting data, these account values with read-only access will not be available to the user.

For rule assignments that are set to **Read and write**, the account values allowed will be applicable in read-only features as well as those features that involve update capabilities for accounting data.

Start Date

Specifies when the user rule assignment begins. The date can't be earlier than the current system date when you're creating a new user rule assignment. This is because a rule assignment can't be effective any earlier than the date when it's created. You can also create a user rule assignment with a future date as the start date.

Note: The start date can't be any earlier than the start date of the policy referenced in the rule assignment.

End Date

Specifies when the user rule assignment ends. This date can't be earlier than the user rule assignment's start date and any later than the end date of the policy referenced in the rule assignment.

You can update the end date on an existing user rule assignment as long as the current end date is today or a date in the future. That is, the rule assignment is still active. The new end date must be at least today's date or a future date, but still within the end date of the policy referenced in the rule assignment. There's no requirement for the new end date to be later than the current end date for the user rule assignment.

For example, let's say today's date is January 27 and the end date for a rule assignment is set to January 31. A day later on January 28, a new end date can be set to January 28 or later as long as it doesn't exceed the end date of the policy referenced in the rule. It doesn't have to be set beyond January 31, which is the original end date. However, you can't update the end date on the rule assignment from January 31 once it's February 1.

For audit purposes, records of segment value security policy assignments to users are never deleted. The rule assignment End Date attribute is used instead to indicate that the policy assignment is no longer applicable.

Related Topics

- Using the Manage Segment Value Security Rules Spreadsheet

Edit Rules and Rule Assignments

To edit existing rules and rule assignments, it's very important, and will always be required, to first download the records from the application.

This ensures that you're working with the current version of the rule or rule assignment that's stored in the application. You can download existing rule and rule assignment records for the secured value set for review or edit by using the Search command on either worksheet on the Manage Segment Value Security tab.

Once you've downloaded the records you want to update, make your edits, and upload your changes to save them to the application. You can also create rules and user rule assignments in the same spreadsheet that you're editing.

On the Rules worksheet, you can filter your search for policies by policy name, segment value security role, or both, by specifying relevant search strings for these fields.

On the Rule Assignments worksheet, you can filter your search for user rule assignments by user name, policy name, or both, by specifying the relevant search strings for these fields.

Best Practices for Creating Segment Value Security Roles

Here are some best practices for creating and maintaining roles for segment value security.

- Create the role solely for the purpose of assigning segment value security policies. This prevents the potential commingling with other elements of data security and other artifacts that might be present in other roles. That could make it much more difficult to diagnose when segment value security rules aren't acting in an expected manner.

  > **Note:** Set the Role Category to **Default**.

- Don't form hierarchies with segment value security roles. Hierarchies could result in the rolling up of data security policies to a user from the various roles within the role hierarchy, based on the assignment of that one segment value security role. This will make it difficult to evaluate the data security a user ends up with, and to identify the precise origin of certain data security policies the user ended up with if unexpected results are encountered.
- It's generally not advisable to use job roles, predefined by Oracle or otherwise, to pass on segment value security policies because it's highly unlikely that a group of users who share a job role will also share the exact same security profile for a secured chart of accounts.

  By attaching segment value security policies to job roles, any user who's assigned that job role will uniformly pick up those data security policies. Job roles are primarily for the purpose of passing function security access to features in a product module, and shared among users who have the same job function, but most likely for different parts of the organization. It's generally best to not incorporate data security access directly into a job role.
- Assess the total number of unique variations of segment value security profiles across all users in the organization who'll need access to a given secured value set. Then, define individual segment value security roles for each of these security profiles by creating empty roles before creating the segment value security policies. The purpose of these roles is to serve as a method to pass through specific chart of accounts segment value security data security policies intended for a given user, or user group, by assigning this segment value security role to the appropriate users.

  Minimize the number of policy definitions that you maintain for a given secured value set by having each policy definition comprehensively capture each of these identified security profiles for that value set. This helps promote a more manageable framework for maintaining the segment value security requirements for your organization.
- Maintaining individual segment value security roles for each distinct data security profile among all the users and user groups in the organization will also help with ongoing maintenance of your segment value security

setups. Any required change to such a segment value security data security profile would only require making a change to the one segment value security role and this will automatically cascade down to all the users that belong to that one security profile.

The one segment value security role can be assigned different policies from within the same secured value set. Even policies from different secured value sets can be assigned, so long as that common security profile applicable to the entire group of users who will share that segment value security role, includes each and every one of these segment value security policies for the one or more secured value sets that will be tied to this segment value security role.

Loading up the one segment value security role can help with cutting down the number of segment value security roles that need to be maintained, and each role can be used very efficiently. However, this can also substantially increase the complexity of organizing and maintaining the segment value security setups by creating additional interdependencies between the security requirements for different policies and different secured value sets, and the security segment value security requirements of each user placed into this group. As such, take caution when loading up a segment value security role in this manner and apply the requisite judgment in weighing the benefits and costs of taking such a decision to determine the optimal fit for your organization.

CAUTION: Don't use the Security Console Role Copy feature to make copies of such segment value security roles that have segment value security policies assigned through policies created using the Manage Segment Value Security Roles spreadsheet. The Role Copy function doesn't account for all the attributes maintained for policy definitions that were created using the spreadsheet. A role created from such a copy action will have data security policy assignments that are incomplete and that won't function properly.

Assign Segment Value Security Roles to Users

For a user to be effectively granted a particular chart of accounts segment value data security policy, that user will need to be assigned the segment value security role tied to that policy.

A working setup to limit access to just certain specific secured account values also requires that the user must have one or more rule assignments for the policy associated with the assigned role. The assignments stipulate under which business function and data access context the policy should be effective for the user, and whether the access level is on a read-only or read and write basis. Otherwise, such a policy can never be actively applied for that user despite the user being assigned its associated role.

When working with a secured chart of accounts segment value set where the user doesn't have a matching rule assignment for a given usage context, that user will have access to all values by default.

Examples of Generic User Rule Assignments for Segment Value Security

To make policies more shareable, you can define generic rule assignments, that is, you define a rule assignment without one or more specific values for the following attributes:

- User Name

- Business Function
- Security Context and Security Context Value

You can select different variations of settings for these attributes to achieve the desired effect of granting access to a user for the secured account values.

Rule Assignments Without a Specified User Name

In this example, you assign three users the same segment value security role.

This is because there are cases where all three users will need access to the same secured account values under the same qualified circumstances of business function, data security context, and access level, which are the attributes of a rule assignment.

The users are CCLARK, LLOPEZ, and PPATEL. They use Oracle General Ledger and are all assigned the same Vision Corporation data access set. The Natural Account segment of the chart of accounts is secured and you define a policy that allows read and write access to all accounts that start with 1. You assign the policy to the shared segment value security role.

This table shows the relevant attribute values on the Rules worksheet.

Attribute	Value
Policy Name	Accounts Start with 1
Policy Description	Natural account segment values start with 1
Role Name	Shared Segment Value Security
Operator	Starts with
From Value	1

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	All users assigned to the role of the policy
Policy Name	Accounts Start with 1
Role Name	Shared Segment Value Security
Business Function	General Ledger
Security Context	Data access set
Security Context Value	Vision Corporation
Access Level	Read and write
Start Date	1-Jan-2024

The User Name for this rule assignment is **All users assigned to the role of the policy**. This indicates that the rule assignment will apply to users CCLARK, LLOPEZ, and PPATEL for the General Ledger business function when using the

Vision Corporation data access set on a read and write basis because they're all assigned the segment value security role Shared Segment Value Security.

Rather than having to define three separate rule assignments for each user, you can structure the rule assignment this way to allow it to be shared and the policy effectively applied to all three users. This streamlines the maintenance of the rule and rule assignment.

Rule Assignments Without a Specified Business Function

It's possible to assign a rule to a user or group of users in a broad manner, where the grant to the secured value is applicable to all business functions that the user or group of users works with.

In this first example, the rule assignment is a broad one, where the user CCLARK can use the Cost Center 100 policy for whatever business function that CCLARK is working with, and for any security context and security context value on a read and write basis.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	CCLARK
Policy Name	Cost Center 100
Role Name	CCLARK Cost Center 100
Business Function	All business functions
Security Context	All security contexts
Security Context Value	All security context values
Access Level	Read and write
Start Date	1-Jan-2024

In this second example, the rule assignment applies to all business functions on a read and write basis, but the user CCLARK is limited to just when the security context is Business unit.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
User Name	CCLARK
Policy Name	Cost Center 100
Role Name	CCLARK Cost Center 100
Business Function	All business functions
Security Context	Business unit
Security Context Value	All security context values
Access Level	Read and write

Attribute	Value
Start Date	1-Jan-2024

Business unit is a relevant security context for the Payables and Receivables business functions. Therefore, this rule assignment would effectively only apply when the user CCLARK is working with those two business functions, and not other business functions like Assets, General Ledger, Provider Intercompany, and Receiver Intercompany, which use a different security context.

Rule Assignments Without a Specified Security Context

The previous topic described a rule assignment example that broadly covered all usage contexts, regardless of the business function, security context, and security context value for the user's usage scenario.

Here are some additional considerations for rule assignments without a specified security context.

This table shows the relevant attribute values on the Rule Assignments worksheet.

Attribute	Value
Business Function	All business functions
Security Context	All security contexts
Security Context Value	All security context values

Because there isn't a single business function where all the different security context types (Asset book, Business unit, Data access set, Intercompany organization) would apply, the **All security contexts** selection for the Security Context attribute of a rule assignment can only work with the **All business functions** selection for the Business Function attribute.

Also, since there likely isn't a single security context value that would be a match for all the different security context types, selecting **All security contexts** for the Security Context attribute for the rule assignment would also automatically mean **All security context values**.

Using Export and Import Services with Segment Value Security by Business Functions Configurations

You need to ensure that the source and target environments for the export and import process are compatible for segment value security.

They must be based on the same segment value security method of either segment value security by business function or segment value security without the business function distinction. Mixing and matching of source and target environments identified with different segment value security methods for such export and import processes will cause data corruptions with the setup configurations in the target environment.

You need to also ensure when using export and import services for segment value security rules and rules assignments from a source to a target environment that the method by which such setup records are created are the same in both environments. Commingling the usage of the Manage Segment Value Security Rules spreadsheet with the Edit Data

Security page or the Rapid Implementation spreadsheet to maintain your segment value security setups will result in serious data inconsistencies that will cause the incorrect enforcement of segment value security.

Enforcement of Segment Value Security by Business Function

These examples illustrate key points about how segment value security by business function enforcement works when using the following types of General Ledger features that involve the chart of accounts:

- Journal entry
- Submission of the predefined Oracle Analytics Publisher Trial Balance Report using the Scheduled Processes page
- Balances cube-based online inquiry using Account Monitor
- Balances cube-based inquiry using Smart View

For all examples, the General Ledger business function has been enabled for security enforcement and the Company, Cost Center, and Natural Account segments of the chart of accounts have been secured. These examples will focus on the segment value security rules for the Natural Account segment. The users in these examples don't have a rule assignment for the Company and Cost Center segments. This means they will have access to all account values based on the default all values access behavior with segment value security by business function.

Here are some more characteristics of the chart of accounts.

- The first segment is the Company segment, the second is the Line of Business segment, the third is the Account segment, the fourth is the Cost Center segment, and the fifth is the Product segment.
- Asset type account values start with 1, Liability type account values start with 2, Owner's Equity type accounts start with 3, Revenue type accounts start with 4, and Expense type accounts start with 5.

There are 3 users: CCLARK, LLOPEZ, and PPATEL. Both CCLARK and PPATEL not only manage the financial accounting for their region, but they're also responsible for calculating the global bad debt reserve. They require full read and write access to all accounts when working with the financial data specific to their assigned region but should have read and write access to just certain accounts for the worldwide financial data related to calculating the global bad debt reserve. For example, PPATEL's configuration mirrors such access requirements with the two data access set assignments.

The following tables provide details on the ledger sets, account access, security profiles, rules, and rule assignments for the examples that follow.

This table lists the ledger sets and their corresponding ledgers.

Ledger Set	Ledgers
Vision Corporation North America	Vision Corporation Canada, Vision Corporation USA
Vision Corporation Global	Vision Corporation Canada, Vision Corporation USA, Vision Corporation Japan

This table describes the Natural Account segment values for the secured chart of accounts that will be used in the rule assignments.

Account or Account Range	Account Description	Parent
12010 - 12999	Bad debt reserve accounts	No
REV	Revenue accounts	Yes
EXP	Expense accounts	Yes
88888	Net Equity All Balance Sheet Accounts	Yes

This table describes the security profile for each user.

User Name	Functional Role	Assigned Data Access Sets	Allowed Accounts	Access Level
CCLARK	General Accounting Manager	Vision Corporation Global	All	Read and write
LLOPEZ	Financial Analyst	Vision Corporation USA	All nonrevenue	Read only
PPATEL	General Accountant	Vision Corporation North America, Vision Corporation Global	All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set	Read and write

The following tables describe the rules and user rule assignments for the secured chart of accounts, Account segment, and Account Vision Corporation value set that were defined to provide access to the users according to their security profile.

This table lists the attribute values that were entered on the Rules worksheet, except for the Policy Description.

Row	Policy Name	Role Name	Operator	From Value	To Value	Tree Code	Tree Version
1	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	Between	12010	12999	This field is blank.	This field is blank
2	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	Is descendant of	REV	This field is blank.	Account Vision Corporation	Account Vision Corporation Current
3	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	Is descendant of	8888	This field is blank.	Account Vision Corporation	Account Vision Corporation Current
4	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	Is descendant of	EXP	This field is blank.	Account Vision Corporation	Account Vision Corporation Current

This table lists the attribute values that were entered on the Rule Assignments worksheet.

User Name	Policy Name	Role Name	Business Function	Security Context	Security Context Value	Access Level
PPATEL	PPATEL Bad Debt and Revenue Accounts	PPATEL Role	General Ledger	Data access set	Vision Corporation Global	Read and write
LLOPEZ	LLOPEZ Nonrevenue Accounts	LLOPEZ Role	General Ledger	Data access set	Vision Corporation USA	Read only

Journal Entry

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic.

It shows how segment value security by business function is enforced for users CCLARK, LLOPEZ, and PPATEL when they're using a transaction entry feature like General Ledger journal entry on the Create or Edit Journal pages.

Let's start with CCLARK. Here's a summary of CCLARK's security profile.

- Assigned Data Access Set: Vision Corporation Global
- Allowed Accounts: All
- Access Level: Read and write

This profile highlights the default grant to all users where they're provided access to all account values on a read and write basis of a secured value set, unless they're assigned a specific rule assignment to limit their access to just certain account values. CCLARK, LLOPEZ, and PPATEL have no rule assignments for the secured Company and Cost Center segments, so they have access to all Company and Cost Center values on a read and write basis This makes it efficient to maintain rules and rule assignments because you only need to maintain such configurations in cases where chart of accounts security enforcement to limit access to just certain secured accounts is required for the user.

CCLARK is on the Edit Journal page, reviewing an unposted journal for the Vision Corporation USA ledger and this table shows the journal line numbers, accounts, and entered amounts that CCLARK can view.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
5	3111-00-40110-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

CCLARK can view every journal line, which reference different Natural Account segment values. With read and write access to all these accounts, CCLARK can also edit the existing lines, add new lines to the journal entry, and create a new journal entry for any account.

Let's now review how this same journal entry would appear to the user LLOPEZ. Here's a summary of LLOPEZ's security profile.

- Assigned Data Access Set: Vision Corporation USA
- Allowed Accounts: All nonrevenue
- Access Level: Read only

This table shows the journal lines line numbers, accounts, and amounts for the unposted journal that LLOPEZ can view.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

Journal line 5 won't display because it's for a revenue account. In addition, LLOPEZ has read-only access to the nonrevenue accounts and can only view the journal information. LLOPEZ can't edit the existing lines, add new lines, or create journals. LLOPEZ also can't select any full account combination because the access granted is only to nonrevenue accounts for the secured Natural Account segment and only on a read-only basis.

Finally, let's review how this same journal entry appears to PPATEL. Here's a summary of PPATEL's security profile.

- Assigned Data Access Set: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set
- Access Level: Read and write

PPATEL has access to the Vision Corporation USA ledger through both data access sets and has different access profiles for each data access set.

Here are some key points.

- A user's access to a secured chart of accounts segment value set can be differentiated, if required, for each business function and security context the user works with. This allows great flexibility in fine-tuning a user's access to secured account values in as specific a manner as required by configuring the rule assignments accordingly.
- The users PPATEL and CCLARK share the same Vision Corporation Global data access set. However, while CCLARK has access to all accounts with that data access set, PPATEL's access is restricted to bad debt and revenue accounts for that same data access set. This highlights the concept that user rule assignments are specific to a given user and the specified data access set in the rule's security context value attribute, in the case of General Ledger.

  A user rule assignment has a set of qualifiers as to when or how the referenced policy will apply, relevant to the specified user. The same notion applies with user rule assignments for the other types of security contexts, such as business units, asset books, and intercompany organization, and their relevant security context values, for their applicable business functions of Payables, Receivables, Asset Books, and Intercompany.

While using the Vision Corporation North America data access set PPATEL can see every line of the unposted journal entry. Moreover, PPATEL can edit any of the journal lines.

This table shows the journal line numbers, accounts, and entered amounts that user PPATEL can view and edit.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
1	3111-00-11010-000-0000	1,000.00	0.00
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-21010-000-0000	0.00	1,000.00
4	3111-00-31001-000-0000	0.00	1,000.00
5	3111-00-40110-000-0000	0.00	1,000.00
6	3111-00-52110-000-0000	1,000.00	0.00
NA	Total	3,000.00	3,000.00

Note: While PPATEL is working with the Vision Corporation North America data access set, this access would be the same with the journals for the Vision Corporation Canada ledger, which is part of that data access set.

While using the Vision Corporation Global data access set, PPATEL's access is limited to the bad debt and revenue accounts and this table shows the journal line numbers, accounts, and entered amounts that user PPATEL can view and edit.

Line	Account	Entered (USD) Debit	Entered (USD) Credit
2	3111-00-12010-000-0000	1,000.00	0.00
3	3111-00-40110-000-0000	0.00	1,000.00
NA	Total	3,000.00	3,000.00

PPATEL can view and edit these journal lines and create journals with the bad debt and revenue accounts.

Note: While PPATEL is working with the Vision Corporation Global data access set, this access would be the same with the journals for the Vision Corporation Canada and Vision Corporation Japan ledgers, which are part of that data access set.

Standard Reports

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic.

It shows how segment value security by business function is enforced for users CCLARK, LLOPEZ, and PPATEL when they're submitting the Trial Balance Report for General Ledger on the Scheduled Processes page.

When users submit the report, they must select one of their assigned data access sets. This selection sets the scope for which ledger the report is to be submitted. For segment value security by business function with a secured chart of

accounts, the data access set is also the basis for determining if there are applicable user rule assignments that would limit the accounts whose balances should be included in the generated report for that user.

The report will be submitted for the same Vision Corporation USA ledger and will focus on the secured Natural Account segment. The users LLOPEZ and PPATEL have user rule assignments that limit access to some natural account values.

Let's start with CCLARK and the summary of CCLARK's security profile.

- Assigned Data Access Set: Vision Corporation Global
- Allowed Accounts: All
- Access Level: Read and write

When CCLARK submits the report for the Vision Corporation USA ledger using the assigned Vision Corporation Global data access set, the report output displays balances for all the natural account values. Having read and write access to secured account values provides CCLARK with the ability to inquire and report on transactions and balances, as well as create transactions and update balances for these accounts.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that CCLARK can view.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00
Total	NA	0.00	130,000.00	130,000.00	0.00

Next, let's look at the report for the user LLOPEZ. Here's a summary of LLOPEZ's security profile.

- Assigned Data Access Set: Vision Corporation USA
- Allowed Accounts: All nonrevenue
- Access Level: Read only

Having read-only access to the secured account values provides the ability to inquire and report on its transactions and balances. The report doesn't include the Revenue account because LLOPEZ's grants to the secured Natural Account segment for the chart of accounts don't include revenue accounts.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that LLOPEZ can view.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00
Total	NA	0.00	130,000.00	70,000.00	60,000.00

Lastly, let's look at the output for the user PPATEL. Here's a summary of PPATEL's security profile.

- Assigned Data Access Set: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America data access set, Bad debt and revenue for Vision Corporation Global data access set
- Access Level: Read and write

When PPATEL runs the report using the Vision Corporation North America data access set, where PPATEL has read and write access to all accounts, the report output displays all the accounts that have balances for the Vision Corporation USA ledger.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that PPATEL can view when submitting the report for the Vision Corporation North America data access set.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
11010	Cash	0.00	90,000.00	0.00	90,000.00
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
21010	Accounts Payable	0.00	0.00	20,000.00	-20,000.00
31001	Common Stock	0.00	0.00	50,000.00	-50,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
52110	Cost of Goods Sold – White Wines	0.00	30,000.00	0.00	30,000.00
Total	NA	0.00	130,000.00	130,000.00	0.00

When PPATEL runs the report using the Vision Corporation Global data access set, where PPATEL has read and write access to the bad debt and revenue accounts, only the balances for those two accounts appear in the report output.

This table shows the accounts, descriptions, and balances on the Trial Balance report for the Vision Corporation USA ledger that PPATEL can view when submitting the report for the Vision Corporation Global data access set.

Account	Description	Beginning Balance (USD)	Debits (USD)	Credits (USD)	Ending Balance (USD)
12010	Bad Debt Reserve	0.00	10,000.00	0.00	10,000.00
40110	White Wine Revenue	0.00	0.00	60,000.00	-60,000.00
Total	NA	0.00	10,000.00	60,000.00	-50,000.00

This example with the user PPATEL illustrates how segment value security rule assignments for a user can be configured in a manner that precisely grants access to secured accounts for a specific data security context value, such as a data access set in the General Ledger module.

Account Monitor Inquiries

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic and focuses on the user PPATEL.

The Account Monitor is an online inquiry tool for reviewing a ledger's account balances.

Users can view summarized account balances rolled up by parent account values and can save their inquiries in the form of account groups. The inquiry results are projected in the Account Monitor. Balances are based on the General Ledger balances cube where balances aggregation is maintained according to the hierarchies for the different data dimensions, including dimensions based on the chart of accounts segments.

Here's a summary of PPATEL's security profile.

- Assigned Data Access Sets: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America, Bad debt and revenue for Vision Corporation Global
- Access Level: Read and write

The account group in this example inquires on a set of account balances for the Vision Corporation USA ledger, with individual natural account values in each row.

When the user PPATEL views the account balances in the Account Monitor using the Vision Corporation North America data access set, all account balances are displayed. This is because PPATL has read and write access to all Natural Account segment values for the secured chart of accounts.

This table shows the account segment values that the user PPATEL can view in the Account Monitor. The Company, Line of Business, Cost Center, and Product columns are excluded from the table because PPATEL has access to all those segment values.

Name	Ledger	Account
Bad Debt Reserve	Vision Corporation USA	12010
Accounts Payable	Vision Corporation USA	21010
Common Stock	Vision Corporation USA	31000
Revenue	Vision Corporation USA	40110
Expense	Vision Corporation USA	52110

When the user PPATEL views the account balances in the Account Monitor using the Vision Corporation Global data access set, only balances from the bad debt and revenue accounts display. This is because PPATEL has read and write access to only the bad debt and revenue Natural Account segment values for the secured chart of accounts.

This table shows the account segment values that the user PPATEL can view in the Account Monitor. The Company, Line of Business, Cost Center, and Product columns are excluded from the table because PPATEL has access to all those segment values.

Name	Ledger	Account
Bad Debt Reserve	Vision Corporation USA	12010
Revenue	Vision Corporation USA	40110

Smart View Inquiries

This example is based on the setup outlined in the *Enforcement of Segment Value Security by Business Function* topic and focuses on the user PPATEL.

It shows how segment value security by business function is enforced in an inquiry tool that's launched outside of the main General Ledger application. Security enforcement is applied just like in the main application, except there are some considerations when the data access set for the user changes.

Smart View is a spreadsheet-based tool for inquiring on General Ledger account balances data that are stored in the General Ledger balances cube. The General Ledger balances cube is where balances aggregation is maintained according to the hierarchies for the different data dimensions, including dimensions based on the chart of accounts segments.

Here's a summary of PPATEL's security profile.

- Assigned Data Access Sets: Vision Corporation North America, Vision Corporation Global
- Allowed Accounts: All for Vision Corporation North America, Bad debt and revenue for Vision Corporation Global
- Access Level: Read and write

When the user PPATEL views the account balances in Smart View using the Vision Corporation North America data access set, all account balances are displayed. This is because PPATL has read and write access to all the secured Natural Account segment values for the secured chart of accounts.

This table shows the accounts and balances that the user PPATEL can view in the Smart View inquiry for the Vision Corporation USA ledger when using the Vision Corporation North America data access set. The point of view for the inquiry includes all values for the Company, Line of Business, Cost Center, and Product segments.

Account	Vision Corporation USA
11010 – Cash	90000
12010 – Bad Debt Reserve	10000
21010 – Account Payable	-20000
31000 – Common Stock	-50000
4011 – Revenue	-60000

Account	Vision Corporation USA
52110 – Expense	30000

When the user PPATEL views the account balances in Smart View using the Vision Corporation Global data access set, only balances from the bad debt and revenue accounts display. This is because PPATEL has read and write access to only the bad debt and revenue Natural Account segment values for the secured chart of accounts.

This table shows the accounts and balances that the user PPATEL can view in the Smart View inquiry for the Vision Corporation USA ledger when using the Vision Corporation Global data access set. The point of view for the inquiry includes all values for the Company, Line of Business, Cost Center, and Product segments.

Account	Vision Corporation USA
11010 – Cash	#No Access
12010 – Bad Debt Reserve	10000
21010 – Account Payable	#No Access
31000 – Common Stock	#No Access
40110 – Revenue	-60000
52110 – Expense	#No Access

When users work with reporting tools for the General Ledger balances cube such as Smart View and Financial Reporting, which are outside of the main application, there's no explicit data access set selection. Users must change the data access within the main application by using the data access set selector or by changing the data access set in General Ledger preferences.

> **Note:** To change the General Ledger preference, use the Set Preferences option on the Settings and Actions menu in the global header.

After changing the data access set, users can click **Refresh** in the Point of View section of the Smart View spreadsheet to register the data access set selection change. For Financial Reporting, users can rerun the report. Taking these steps ensures that the correct segment value security grants are applied to the reports with these reporting tools based on the current data access set selection.

Special Considerations for Segment Value Security

There are special considerations for segment value security by business function in the following areas:

- Back-end processes
- Setup tasks
- Oracle Transactional Business Intelligence reporting
- Features without a specific data security context
- Multiple secured chart of account segments

- Primary balancing segment value assignments to a ledger or its legal entities
- Switching from secured to unsecured modules

Back-End Processes

Segment value security by business function isn't enforced for back-end processes.

Back-end processes are submitted processes that run in the background without active engagement from users. Some of these processes can generate or update financial data that's framed by chart of account values like accounting transactions and account balances.

This table provides examples of such back-end processes.

Module	Back-End Processes
General Ledger	Posting, Translation, Revaluation, Open Period
Subledger Accounting	Create Accounting

Note: While reports on financial data are also submitted for processing, they aren't considered back-end processes. They're requests to display financial data in an output format.

Segment value security by business function isn't enforced for such back-end processes for these reasons.

- As accounting becomes more automated, administrators are more likely to submit back-end processes on behalf of end users, who work with the financial data resulting from these processes.
- In some cases, the application itself might initiate the submission of the back-end process.
- The user submitting back-end processes might be detached from the end users who will ultimately work with the resulting financial data.
- There might be a lack of direct correlation between the back-end processes and the security profiles of the users submitting these processes.

The key to securing financial data is to ensure that end users should only be able to access the financial data that they're authorized to work with. As such, enforcement of segment value security by business function is strictly applied when such users update financial data, or report or inquire on it.

Setup Tasks

Segment value security by business function isn't enforced for setup tasks.

Some setup tasks are related to the configuration of application or processing rules that produce accounting transactions and financial data. Such setup tasks often touch on elements of a chart of accounts and include configurations and mapping rules that drive what chart of account values will be used when the financial data is generated.

Access to such setup tasks, especially around setting up reference data, is typically granted only to an administrator job role, where users assigned that role would be responsible for configuring the application. These users don't work directly with the financial data itself.

In addition to reference data setup, these tasks also include transaction generation setups, which can directly generate accounting or journal entries.

Here are some examples.

- Assets: Asset book definition
- General Ledger: Allocation formulas
- General Ledger: Chart of accounts configuration
- General Ledger: Chart of Accounts Mapping rules
- General Ledger: Ledger definition
- General Ledger: Revaluation definitions
- Intercompany: Balancing Account rules
- Receivables: AutoInvoicing rules
- Subledger Accounting: Create Accounting rules
- Subledger Accounting: Transaction Account Builder rules

Setup tasks typically don't have a selection for a security context value, such as a data access set, business unit, asset books, or intercompany organization, for the purposes of establishing the data security element while working on the setup record.

If such security context objects were referenced, it's for the purpose of identifying which instance of that object the setup is being configured for, rather than about creating financial data with that security context value.

The administrator, or the user provided functional access to work with such setup tasks, can set up configurations and accounting rules across all ledgers, business units, asset books, and intercompany organizations in the application. A setup administrator user can use any account value, even for a secured chart of accounts value set. Access to the setup tasks alone allows the user to work with any of such setup records without further data security enforcement.

Oracle Transactional Business Intelligence Reporting

For segment value security with Oracle Transactional Business Intelligence (OTBI) reporting, enforcement by business function isn't supported.

Once a chart of accounts value set is secured, security will be enforced across all business functions, regardless of whether each distinct business function is enabled for enforcement or not. So long as the value set is security enabled, security enforcement will apply in all business functions of General Ledger, Payables, Receivables, Assets, Intercompany, and Subledger Accounting.

With OTBI reporting, it's possible to put together reports that cross multiple products (business functions). Moreover, the user doesn't directly select which data access security context (Data Access Set, Business Unit, Asset Books, and so on.) to currently work with. Instead, in general, the user's cumulative data access security assignments are always simultaneously taken together. Both of these factors affect the ability to precisely and fully apply segment value security by business function.

When performing OTBI reporting with the General Ledger subject area specifically, the user's current data access set selection determines the applicable data security. This is because the user's currently selected data access set in the application is stored in a profile option. The application leverages this and singularly applies it in evaluating which segment value security user rule assignments should apply for the user when reporting on ledgers with a secured chart of accounts. When reporting on ledgers that don't have a secured chart of accounts, the user's cumulative assigned data access sets are simultaneously applied.

Features Without a Data Security Context

There are product features that involve working directly with financial transactions and balances where a user's data security context can't be established.

Here are some examples.

- Standard Subledger Accounting Oracle Analytics Publisher reports that can involve the financial data of one or more ledgers where there isn't always a direct or unique match to a specific security context value that's assigned to a user, such as a data access set.
- Non-General Ledger Oracle Transactional Business Intelligence reports where no specific data security context selection can be established for a user to derive the specific segment value security by business function grants that are applicable to that user.

For these features, a modified form of segment value security by business function enforcement is applied. A percentage value is substituted for certain user rule assignment attributes to indicate that no specific value needs to be matched for the security grants. This broader basis of user rule assignment matching still limits a user's access to the secured accounts that the user is granted access to when working with financial data, but on a nonspecific basis.

Here's how it works for such features.

When determining if there are matching rule assignments for a user that can restrict the range of accessible secured accounts, the Security Context and Security Context Value attribute settings will be ignored to lower the matching threshold. The Business Function and Access Level attributes for that rule assignment can still be considered.

This would be in place of automatically applying the All Values grant when no precise user rule assignments match for the current usage scenario. That approach would effectively mean that no chart of accounts security would be enforced. Instead, this alternative approach will at least limit a user to working with only the financial data where the cumulative grants for each secured value set of the chart of accounts provide access, should such grants exist.

As another example, when working with features in the Subledger Accounting application, a user doesn't explicitly specify a security context selection (that is, a data access set, business unit, and so on). With General Ledger, that same user can simultaneously work with the financial data of ledgers across the user's cumulative data access set assignments.

This means that for those security grants for a user that can be tagged with a specific security context value, such as a data access set, it isn't possible to make perfect matches of the user's more precisely defined rule assignments for the usage scenario in Subledger Accounting. If it happens that such grants are tagged with the All Security Contexts security context, or the Data Access Set security context paired with the All Security Context Values security context value, such grants for the user are also included as a match.

For a General Ledger user, all the user's General Ledger business function rule assignments for the secured value sets involved with the charts of accounts of the ledgers that user is working with will also be applied. This is regardless of the data access set security context and security context value that's associated with those rule assignments. That is, all the user's General Ledger business function rule assignments for the secured value sets will be cumulatively applied. If under such looser matching conditions there are still no matching grants for the user, only then will the default All Values grant to the relevant secured value sets apply.

Multiple Secured Chart of Account Segments

Consider these points when working with account combinations where the chart of accounts has multiple segments enabled for segment value security by business function.

- For a given usage scenario, a user's access to the account values of each secured chart of accounts segments is first considered individually and independently of the other. Then, if a user has a mixture of access levels to the account values for an account combination, the lowest level of access among these account values would be applied to the full account combination.
- For an account combination where a user has no access to at least one segment's account value, that account combination is immediately one to which the user has no access. This is because access to the account combination requires access to each of its secured segment values.

- For an account combination where a user has read-only access to at least one segment's account value, that account combination is a read-only account combination for the user. This is because read and write access to an account combination requires read and write access to each of the account combination's secured segment values.

As an example, the first and second segments of account combination 01-101-1000 are secured. A user has read-only access to first segment value 01 and no access to second segment value 101. The user won't have access to that account combination. Even if the user had read and write access to first segment value 01, the user still wouldn't have access to account combination 01-101-1000.

Continuing with this example, a different user has read-only access to first segment value 01 and read and write access to second segment value 101. That user's applicable access level to account combination 01-101-1000 will be read only.

To have read and write access to account combination 01-101-1000, a user must have read and write access to both first segment value 01 and second segment value101.

If a user doesn't have at least read-only access to accounts on every secured segment of an account combination, that user won't even have read-only access to that account combination.

Primary Balancing Segment Value Assignments to a Ledger and Its Legal Entities

Assigning a primary balancing segment value to a ledger, or to its legal entities, isn't chart of accounts data security related.

It's a validation against the accounting configuration for a ledger that affects which primary balancing segment values are available and valid for a user to work with for the given ledger.

If a ledger has primary balancing segment value assignments and a particular primary balancing segment value isn't assigned to that ledger, or to its legal entities, then that primary balancing segment value won't be available to the user when working with that ledger. This is regardless of whether the user has been granted access using either of the following methods:

- The user is provided a segment value security grant for that particular primary balancing segment value for that chart of accounts with a secured primary balancing segment.
- The user is granted access to that primary balancing segment value through a full ledger data access set or a primary balancing segment value-based data access set, in the case of the General Ledger module.

Switching from Secured to Unsecured Modules

When users switch from one of the modules that support segment value security by business function to a module that doesn't, they might continue to experience limited account access in the unsecured module.

To resolve this, users might need to sign out of the application and sign back in when switching modules. This action resets the cache and allows users access to all accounts in those modules where security enforcement isn't expected.

General Ledger-Specific Considerations for Segment Value Security

Segment value security by business function is generally enforced in General Ledger product features with a chart of accounts element and where a single data access set context selection can be clearly established for a user's session.

In these cases, the secured account values available to the user, at the according access level, are based on those grants assigned to the user for the General Ledger business function and the user's current selected data access set.

Here's a summary of how segment value security by business function works for General Ledger features that have different types of derivation of the user's data access set selection.

- For features accessed directly in the core application, a user would select a data access set. The selection also sets the data security context when determining which of the user's segment value security by business function grants apply when working with the secured chart of accounts.

  > **Note:** The data access selection is also registered in a user's General Ledger preferences for the Data Access Set General option.

- For features accessed outside of the core application, where a user doesn't explicitly select a data access set, such as with reporting tools Smart View, Financial Reporting, and Oracle Transactional Business Intelligence (OTBI), the application refers to a user's last selected data access set in the core application when determining which of the user's security grants apply.

  > **Note:** If a user switches data access set selection in the core application, it's important to refresh the view in the Smart View, Financial Reporting, and OTBI reports. This action registers the change in data access set selection so that the relevant set of security grants based on this new data access set selection is now applied to the report.

- For features where multiple data access sets can apply, or where no data access set context can be established, there are some other considerations regarding how segment value security by business function is enforced. Some examples in the *Features Without a Data Security Context* topic discuss some of these considerations.

Further details follow about other special considerations for data security and segment value security by business function enforcement in certain features in the General Ledger module. They elaborate on certain points discussed previously, as well as other specific aspects of security control in the General Ledger module.

Data Access Sets

For General Ledger, data access sets provide users with access to one or more ledges and serve as a core and required data security mechanism.

Data access sets are a fundamental data security control object that always apply in General Ledger and are unique to the General Ledger module. They include the following attributes:

- Access Set Type
- Access Level

Here are the access set types.

- Full Ledger: This type provides access to an entire ledger. It can include one or more ledgers as well as ledger sets. When a ledger set is added to a Full Ledger data access set, access to all the ledgers in the ledger set are granted in full.

  Whenever a new ledger or ledger set is created, the application automatically creates an implicit data access set for it. This data access set can't be updated. An explicit data access set can also be created for one or more ledgers, or ledger sets, or both. Explicit data access sets are updatable.

- Primary Balancing Segment Value: This type provides access to one or more primary balancing segment values of a ledger or ledger set.

  You can specify a single or parent value. If you specify a parent value, the data access set provides access to all the single values that roll up to that parent value. The parent value is evaluated based on the current version of the hierarchy associated with the primary balancing segment in the chart of accounts definition.

Here are the access levels.

- Read Only

  > **Note:** Even if a user carries the functional privilege to use certain write-level functions, such as the ability to create a journal, the user will be prevented from taking any action that will update General Ledger transactions and balances for a given ledger or primary balancing segment value.

- Read and Write

Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment

For segment value security by business function, data access sets serve as the security context basis for the General Ledger module.

For the Subledger Accounting module, to the extent that there's a touchpoint with the General Ledger module, the data access set also plays an indirect role in establishing a user's data security and it's used to establish a user's ledger and ledger set access scope.

If you enable segment value security by business function for the value set of a chart of accounts primary balancing segment and also use the data access set type of Primary Balancing Segment Value, the two data security control elements, including their access levels, will apply to those primary balancing segments in General Ledger.

> **CAUTION:** The recommended best practice is not to use both methods because having dual levers of control on access to the one element of the chart of accounts primary balancing segment can introduce unneeded complexities, ambiguity, and inconsistencies.

Instead, limit the implementation of data security control of primary balancing segment values to one of these two methods:

- Data access sets with an access set type of Primary Balancing Segment Value
- Segment value security by business function enabled on the primary balancing segment of the chart of accounts.

Here are some guidelines on which of the two methods to use.

- If security on the primary balancing segment of the chart of accounts will always only be required in the General Ledger module, then use Primary Balancing Segment Value-based data access sets alone to specifically control primary balancing segment values access in General Ledger. Data access sets and Primary Balancing Segment Value-based data access sets are unique in usage for data security control in the General Ledger module.
- If security on the primary balancing segment of the chart of accounts is also required in other product modules besides General Ledger, then enable segment value security by business function on the primary balancing segment of the chart of accounts. This is the only option that applies to all product modules. Avoid using Primary Balancing Segment Value-based data access sets for General Ledger in this case and only use the Full Ledger access type of data access sets.

How Data Security Works When Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment

If you don't follow the recommended best practice described in the *Using Primary Balancing Segment Value-Based Data Access Sets with a Secured Primary Balancing Segment* topic, and instead use both Primary Balancing Segment Value-Based data access sets along with a secured primary balancing segment, here's a summary of how data security works followed by examples.

For features directly based on the General Ledger balances cube, a user's access to primary balancing segment values will be based on the cumulative union of the two data security control methods.

For features indirectly based on the General Ledger balances cube, a user's access to primary balancing segment values will be based on the intersection of the two data security control methods.

Example of Primary Balancing Segment Value Access for Features Directly Based on Balances Cubes

Most balances cube-based features in General Ledger pertain to reporting or inquiry functions. That is, they're read-only type functions. For read-only features, the rules assigned to a user on both a read-only and read and write basis will apply.

The following General Ledger features are directly based on General Ledger balances cube.

- Account Groups and Account Monitor
- Account Inspector
- Allocations
- Close Monitor Summary Income Statement
- Correct Budget Import Errors
- Create Budgets in Spreadsheet
- Financial Reporting
- Inquire and Analyze Balances
- Inquire and Analyze Average Balances
- Inquire on Detail Balances
- Oracle Transactional Business Intelligence (OTBI): General Ledger Balances Real Time and Average Daily Balances Real Time Subject Areas
- Revenue, Expenses and Allocations Infolets
- Smart View

From this list, only Allocations, Create Budgets in Spreadsheet and Correct Budget Import Errors are features that are of a read and write nature. Segment value security enforcement won't be applied for them. These features have an element of import and are considered more like back-end processes.

For features that are based directly on balances cubes, a user can access the cumulative primary balances segment values that are granted through both of these methods:

- The user's primary balancing segment value-based data access set.
- The user's applicable rule assignments to the secured primary balancing segment value set.

The application evaluates each method separately. It determines which ledgers a user has access to based on the data access set, as well as the primary balancing segment values granted in the case of Primary Balancing Segment Value-based data access sets. It then separately determines which primary balancing segment values a user has access to for

the secured primary balancing segment based on that user's applicable segment value security by business function grants.

The result is that a user gets access to the cumulative primary balancing segment values from the data access sets and segment value security by business function grants across all ledgers and ledger sets included in those data access sets.

Here's an example.

This table shows the access set assignments for the Vision Corporation Global data access set. This access set has a type of Primary Balancing Segment Value.

Ledger or Ledger Set	Type	Specific Value	Segment Value	Privilege
Vision Corporation Global	Ledger	Single Value	3111	Read and Write
Vision Corporation Global	Ledger	Single Value	3121	Read Only

Note: The All Values, Tree Code, and Tree Version Name fields don't have values, so they're excluded from the table.

This table shows the key attribute values on the Rules worksheet for the secured value set of the Company primary balancing segment.

Policy Name	Role Name	Operator	From Value
CCLARK EQ 3111	CCLARK Role	Equal to	3111
CCLARK EQ 4888	CCLARK Role	Equal to	4888

This table shows the key attribute values on the related Rule Assignments worksheet.

User Name	Policy Name	Role Name	Business Function	Security Context	Security Context Value	Access Level
CCLARK	CCLARK EQ 3111	CCLARK Role	General Ledger	Data access set	Vision Corporation Global	Read and write
CCLARK	CCLARK EQ 4888	CCLARK Role	General Ledger	Data access set	All security context values	Read and write

When user CCLARK uses Smart View to inquire on the Vision Corporation Global ledger's account balances, CCLARK can see company values 3111, 3121, and 4888. Because CCLARK is performing a read-only action, the read-only access level for company 3121 is enough for the inquiry. For any other company values, Smart View will display #No Access.

Note: One exception to this cumulative behavior is when segment value security by business function rules grant access to all primary balancing segment values, but the Primary Balancing Segment Value-based data access set only provides access to select primary balancing segment values. In this case, the restricted access of the data access sets to just select primary balancing segment values will apply, because distinct primary balancing segment values were specified for the data access set.

Example of Primary Balancing Segment Value Access for Features Not Based on Balances Cubes

All General Ledger features that aren't specifically mentioned in the *Example of Primary Balancing Segment Value Access for Features Directly Based on Balances Cubes* topic are associated with relational database tables.

Using the data access set and rules setup from the previous example, when the user CCLARK selects the Vision Corporation Global data access set in a General Ledger feature that's not based on the balances cube, the only primary balancing segment value that CCLARK can work with is 3111. That's because value 3111 is the only primary balancing segment value that’s granted in both the Primary Balancing Segment Value-based data access set and in the segment value security by business function assignment.

When reviewing and editing a journal entry using that same data access set, the user CCLARK will see only the journal lines with account combinations that refer to Company 3111.

> **Note:** A user can edit journal lines only when the assignments for a Primary Balancing Segment Value-Based data access set cover all the primary balancing segment values that are referenced in the account combinations for all journal lines.

Read-Only Data Access Sets with Segment Value Security

When working with read-only data access sets at the ledger level, the entire ledger is read-only for a user.

Having read and write access to account values to any secured segments of its chart of accounts would be irrelevant. The access level to those accounts in that ledger will effectively still be read only because the user’s access to that whole ledger, per the data access set, is read only.

Reporting on General Ledger Balances Cubes Reports with Account Hierarchies

General Ledger balances cubes are differentiated by unique combinations of a chart of accounts and an accounting calendar.

Balances cubes maintain summarized account balances for all trees and tree versions, and for all chart of account dimensions that are published to those balances cubes. The detail account balances for those published trees and tree versions are summarized according to defined account hierarchy rollups.

Trees and tree versions are defined in the application to represent date effective versions of account hierarchies. They’re organized for different purposes, for example, for statutory versus management reporting, with each tree version being assigned an effective date range.

However, this date effectivity isn’t an actual attribute in balances cubes. Instead, it’s an implied characteristic. Users need to know the significance of each tree and tree version that they select and which effective date of the organization’s rollup those tree versions represent. This helps facilitate performing year-over-year comparisons of financials results.

For example, this user-determined control allows organizations to report on fiscal year 23 versus fiscal year 22 financial results using the same tree version rollup for parent account values on both sets of numbers so that there's a consistent comparison between them.

A user can have a choice of reporting on both years' results using last year's tree version rollup for parent account values, or both using the current year's tree version rollup. They can even report on fiscal year 22 results using the fiscal year 22 rollup with the fiscal year 23 results using the fiscal year 23 rollup, if that's what’s required.

Segment Value Security Rules Based on Account Hierarchies

You can refer to account hierarchies in segment value security by business function policies as an efficient way of granting access to secured account values.

Use the hierarchical operators **Is descendant of** and **Is last descendant of**, along with a specified tree, to allow references to parent account values in a security rule condition. This means that a grant provides access to that parent value and all its descendants (with the **Is Descendant of** operator) or to that parent and its' detail values descendants (with the **Is last descendant of** operator), according to the account hierarchy that's defined for the applicable tree code and tree version.

> **Note:** The trees that you specify in a rule must be flattened. This contrasts with trees that are published to balances cubes, which don't need to be flattened. If your security rules refer to trees that are published to the balances cubes, then the trees must be flattened. Otherwise, security enforcement won't work in balances cube-based reports and queries.

While a distinct tree code is associated with each segment in a chart of accounts, as specified through the Default Hierarchy value in the chart of accounts structure setup, a security rule can refer to any tree (hierarchy) that's defined for the secured value set.

The tree version that you specify in a rule is just for the purposes of determining which parent values you can select from to then attach to the security rule condition. At runtime, the application applies date effectivity to identify the version of the tree referenced in the rule whose effective dates intersect with the current system date. Based on this tree version, the application derives the list of accessible descendant account values for the referenced parent value of that tree that are granted by that hierarchical security rule assignment.

For inquiring and reporting in balances cubes, these security grants apply across all versions of the specified hierarchy, as well as all hierarchies associated with the same value set of the specified hierarchy that are published to the GL balances cube. Even though a security rule has a specific tree and tree version for a parent value, the derived set of account values granted by that rule will equally apply to all other published tree and tree versions for where that same parent value is cited and as indicated in GL balances cube-based inquiries and reports.

This example highlights that the grant for segment value security rules based on hierarchies will apply the current effective tree version when deriving the list of accessible values. This contrasts with references to tree and tree versions in balances cube inquiries and reports, where a user controls exactly which tree and tree version they want to use for a rollup.

This table shows the hierarchies, hierarchy versions, parent value, and parent value descendants for this example.

Hierarchy	Hierarchy Version	Parent Value	Parents and Detail Value Descendants
Management	2023	100	• Detail 101 • Parent 200, with detail values 201, 202, 203 • Parent 300, with detail values 301, 302
Management	2024	100	• Parent 200, with detail values 101, 201, 202 • Parent 300, with detail values 301, 302

Hierarchy	Hierarchy Version	Parent Value	Parents and Detail Value Descendants
Geographical	2023	100	• Parent 200, with detail value 201 • Parent 300, with detail values 301, 302 • Parent 400, with detail values 401, 402

Let's say a rule is defined with these attributes.

- Operator: Is descendant of
- From Value: 100
- Tree Code: Management
- Tree Version: 2023

Here's how the application determines the secured values granted.

1. The application derives the hierarchy (tree) version that's in effect based on the current system date, which is January 1, 2024. In this example, that's version 2024.
2. The application then applies the rule condition to get the list of secured values. In this example, the secured values granted are 100, 200, 101, 201, 202, 300, 301, and 302 (parent value 100 and all its descendants in tree version 2024.)
3. This list of values will be accessible across all versions of the Management hierarchy and across all hierarchies associated with the value set for the segment. This means the list of values will be accessible if choosing to report against any version of the Management or Geographical hierarchies.

> **Note:** Value 203 in Management hierarchy version 2023 and values 400, 401, and 402 in Geographical hierarchy version 2023 won't be accessible because they aren't part of the effective 2024 tree version for the Geographical hierarchy.

For the purpose of data entry, this date-effective list of accessible descendant segment values is available to the user for that given point of time.

For the purpose of inquiry and reporting with the balances cube, the same list of accessible descendant segment values is available to the user for all published trees and tree versions for the secured value set of the chart of accounts segment or dimension. Based on the tree and tree version the user selects, the balances data for the accessible descendant segment values of the referenced parent account will be displayed accordingly. A user can also be granted access to a specific parent value. In that case, the summarized balance shown for that parent value will be consistent with the rollup for the selected tree and tree version for reporting purposes, regardless of whether the user has been granted access to all the descendants involved with that particular rollup.

> **Note:** No chart of accounts security is applied during the selection process of account values for the inquiry or report. The user can freely select any dimension member or account values from a secured value set. Security is applied only when retrieving the results for that query or report, and only the balances data of the dimension member or accounts to which the user has access will be displayed.

The advantage of the application dynamically applying date effectivity to security rules is that the rule would be self-maintaining. This methodology works well when it comes to creating transactions or financial data, which in most cases is a real-time exercise.

For comparative reporting, such as with year-over-year financial reporting, previous tree versions might be used as the basis of the rollup to compute summarized balances. This might result in some discrepancy in the access to the descendant accounts for that parent based on the previous tree version's rollup as referenced in the inquiry or report. A potential solution would be to use a different hierarchy in the security rule that encompasses all the account values the user will need to inquire or report on, and give access on a read-only basis to limit the user's ability to enter transactions with these account values.

Considerations When Using Parent Account References in Hierarchical Rules for Balances Cubes

Ensure users get the appropriate secured values grants to view the financial data that they need.

A good practice is to define hierarchical rules that sync to parent values according to the tree as referenced in balances cube inquiries and reports such as Account Monitor, Smart View, and Financial Reporting.

Access to the descendant accounts of a specific parent value should be in sync with the descendant accounts that roll up to the summary account balance of that parent value based on another tree. Otherwise, the parent value will show the appropriate summary balance for the other tree, but the detail breakdown shown on the report of its descendants' balances might not sum up consistently because of lack of access to those descendant values.

This concern applies even when the tree referenced in inquiries and report definitions is the very same one used in the security rule with parent value references. This is because there can be a difference in the dynamic date-effective version rollup that's applied when determining the grants for the rule assignment. Moreover, it's even possible to use a different tree in inquiries and report definitions than the one used in the rule, which can result in even more pronounced disparities.

Journal Approval

With journal approval, the primary consideration when it comes to what a user can access is the approval hierarchy and whether the user is the authorized approver for a given transaction.

It's less about the approver clearing the data access set and chart of accounts segment value security access for the journal batch being approved.

> **Note:** Approval transactions can be reassigned, delegated, and so on, as per the approval rules.

There are differences in the degrees of data security enforcement in the variety of methods for accessing approval notifications and journal batch details in which a user's data access is validated. The most stringent access is where the approver interacts with the journal batch being approved in the context of the Journals page, where all the General Ledger data security elements are directly in place.

These considerations are equally relevant regardless of whether segment value security by business function is enabled.

Back-End Processes That Generate Journals or Update Balances

Segment value security by business function isn't enforced for back-end processes. This is to facilitate automated submission of such processes.

Here are the General Ledger back-end processes that involve a chart of accounts element and that generate journals or update account balances.

- AutoPost Journals
- Create Balance Sheet Closing Journals
- Create Income Statement Closing Journals
- Encumbrance Year End Carry Forward

- Import Journals
- Journal propagation from a primary to a secondary ledger
- Open General Ledger Periods
- Revalue Balances
- Transfer Balances to Secondary Ledger
- Translate General Ledger Account Balances
- Transfer Ledger Balances

Feature Setups

Segment value security by business function isn't enforced for setup tasks.

This table shows examples of General Ledger setups and related processes, spreadsheets, and templates for which segment value security by business function isn't enforced.

Setup	Related Processes	Related Spreadsheets	Related File-Based Data Import Template and Web Service
Account Combinations	Import Account Combinations	Create Account Combinations in Bulk	Import Account Combinations, Account Combinations for Validation
Create Allocation Rules	Generate Allocations	NA	NA
Cross-Validation Combination Sets	Manage Account Combination Validation Rules	NA	Cross-Validation Combinations Import
Cross-Validation Rules	NA	Create Cross-Validation Rules in Spreadsheet	NA
Ledger Options	NA	NA	NA
Segment Values and Hierarchies	Import Segment Values and Hierarchies, Inherit Segment Value Attributes	Rapid Implementation for General Ledger	Import Segment Values and Hierarchies
Segment Value Security	NA	Manage Segment Value Security Rules, Create Segment Value Security Rules	NA
Suspense Accounts	NA	NA	NA

Assets-Specific Considerations for Segment Value Security

Asset books control data security and are the fundamental data security object in Oracle Assets.

It serves as the primary control for an Assets user with access to work with the records of a particular asset book, based on the user's access assignment. This includes the ability to work with and perform actions in an asset book like adding assets, editing asset source lines, entering unplanned depreciation, transferring assets, running Assets reports, and performing inquiry on asset records and transactions.

Chart of accounts segment value security is another layer of data security above asset books that controls a user's ability to work with the chart of accounts-based accounting information of records in a given asset book.

Segment value security restricts access to account segment values in transactions with the Accounting flexfield component in transactions like asset additions and asset transfers. It doesn't restrict transaction entry for an asset within the asset book that doesn't involve the chart of accounts element.

Users who don't have access to segment values used in the accounting for an asset record can still search for that asset record in all the transaction entry and asset inquiry pages in the asset books they have access to. Only when they're working on the chart of accounts-based accounting aspect of an asset record will segment value security access controls be applied. You can only work with account values in a secured chart of accounts value set you've been granted access to through your rule assignments.

Segment Value Security by Business Function for Oracle Assets

The Segment Value Security by Business Function feature lets you enable security enforcement for all business functions or for one or more specific business functions.

For example, you can enable segment value security enforcement for the Oracle Assets business function alone.

When you enable security enforcement for Assets, all Assets users automatically have access to all segment values until you specifically restrict access for one or more users to limited segment values.

You only need to maintain segment value security rules and rule assignments for users who must have access to limited account values by using the Manage Segment Value Security Rules spreadsheet.

For example, you can define the following types of segment value access rule assignments for Assets users who require access to certain secured account values:

Access Type	Business Function	Security Context	Security Context Value
Global access	All business functions	All security contexts	All security context values
Access for Assets business function only	Assets	Asset book	All security context values
Access for specific asset book	Assets	Asset book	Name of asset book

Assign the access type according to the type of access each user needs:

- Global access: Assign to users with responsibilities in multiple business functions such as Assets, Oracle Payables, and Oracle General Ledger, and who require access to the same specified segment account values for all their assigned asset books, business units, and ledgers.
- Access for Assets business function only: Assign to users with only Assets responsibility who require access to the same specified segment account values for all their assigned asset books.
- Access for specific asset book: Assign to users with only Assets responsibility who require access to the specified segment account values for a specific asset book.

Generally, you should create dedicated segment value security roles for data security policies to grant access to secured segment account values to Assets users. Never directly create segment value data security policies with job roles such as Asset Accountant or Asset Accounting Manager, because these roles are likely to be shared among all Assets users, and these users are likely to have different chart of accounts segment value security profiles. The dedicated segment value security roles with their secured segment values can be assigned and even shared with the corresponding users based on their particular segment value access requirements.

Secured segment account values can be granted with these access levels:

- Read and Write: Provides access to create, update, view accounting for, inquire on, and report on Assets transactions that reference the account values granted.
- Read Only: Provides access to view accounting for, inquire on, and report on Assets transactions that reference the account values granted.

Segment Value Security Enforcement in Assets Transactions

Segment value security is generally enforced in Oracle Assets in transactions that directly include the chart of accounts element.

It has no impact on transactions in which actions don't directly involve the chart of accounts, such as cost adjustments, category changes, source line transfers, and suspend or resume depreciation transactions. When searching in pages such as the Adjust Assets and Asset Inquiry pages, it retrieves all asset records without regard to the account values referenced in the distribution lines associated with each asset, and only considers the asset book's element of data security control.

Segment value security is enforced in Assets as follows:

- Users with read and write access to certain account values can take these actions on asset records that reference those account values:
  - Add an asset
  - Prepare source lines
  - Record unplanned depreciation
  - Transfer an asset
  - Make unit adjustments
  - Create a lease
  - Change the financial terms of a lease
- Users with read-only access to certain account values can take these actions on asset records that reference those account values:
  - View distributions and accounting lines
  - Run reports
- Segment value security isn't enforced:
  - In Assets setup pages, such as Manage Assets Books, Manage Asset Categories, and Manage Distribution Sets, even though these pages involve the chart of accounts element.
  - For submitted processes such as Post Mass Additions and Create Accounting.

Example of Segment Value Security by Business Function

The following setup example illustrates how enforcement by segment value security by business function works in Oracle Assets.

You must assign the rules to users for them to have access to the secured account values. If no rules are assigned to a user, the user has access to all the account values.

In this example, user SANJAY has no rule assignments; SANJAY has access to all secured rule account values for the asset books SANJAY has access to.

User KUMAR has access to two asset books: FIN CONSULTING CORP and HR CONSULTING CORP. This table shows the access setup for KUMAR.

User	Role	Business Function	Asset Book	Security Context Value	Access Level
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	HR CONSULTING CORP	3111, 3888	Read and Write
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	FIN CONSULTING CORP	3121, 3999	Read and Write
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	HR CONSULTING CORP	3121, 3999	Read Only
KUMAR	FA_SVSBF_CUSTOM_ROLE	Assets	FIN CONSULTING CORP	3111, 3888	Read Only

Asset additions:

For the write action of asset additions, in the book HR CONSULTING CORP, KUMAR has read and write access to company 3111 and 3888. Therefore, KUMAR can add assets using these account values for that asset book. KUMAR also has read only access to the companies 3121 and 3999. Even though KUMAR has read access to these values, KUMAR can use only 3111 and 3888 to perform asset additions in this book.

In the asset book FIN CONSULTING CORP, KUMAR has read and write access to the companies 3121 and 3999. Therefore, KUMAR can add assets using these account values.

Edit source lines:

In the asset book FIN CONSULTING CORP, KUMAR has read and write access to the companies 3121 and 3999. KUMAR can edit the Depreciation Expense Account using the accounts KUMAR has read and write access to.

In the book FIN CONSULTING CORP, KUMAR has read-only access to company 3888. KUMAR can't edit this depreciation expense account and can only view it.

Transaction Account Builder in Assets:

In Assets, segment value security isn't enforced in the Transaction Account Builder, which is used to drive the depreciation expense account for mass addition lines. This process defaults accounts based on the rules configured by the organization and isn't subject to the limitations of a user's secured account grants.

Asset transfers:

In the book FIN CONSULTING CORP, KUMAR has read and write access to company 3999. Therefore, KUMAR can transfer the asset that references that account in the FIN CONSULTING CORP asset book.

In the book FIN CONSULTING CORP, KUMAR has no access to company 4111 and has read and write access only to the values for company 3121 and 3999. Therefore, KUMAR can't transfer an asset that references values in company 4111.

Example of Accounting in Oracle Assets

In the asset book FIN CONSULTING CORP, among the accounts user KUMAR is granted, KUMAR has read and write access to company 3999 and read-only access to company 3111.

Therefore, when viewing accounting lines for asset records, KUMAR can view all lines that reference accounts KUMAR has read and write and read-only access to.

In the asset book FIN CONSULTING CORP, any user other than KUMAR, who's assigned rules that don't include 3111 and 3999, can't view these accounting transactions.

Example of Reports in Oracle Assets

In the book FIN CONSULTING CORP, KUMAR has read and write access to companies 3121 and 3999, and read-only access to companies 3111 and 3888.

Therefore, KUMAR can report on asset records that reference these four account values for that asset book. KUMAR can't run reports for any values other than those that KUMAR has read and read and write access to.

Intercompany-Specific Considerations for Segment Value Security

These are some considerations for the Segment Value Security by Business Function feature in the Intercompany module.

- Intercompany organization is used as the data access security object in the Intercompany module.
- For the Segment Value Security by Business Function feature, the Intercompany module supports these two distinct business functions:
  - Provider Intercompany
  - Receiver Intercompany

This allows for different security grants to be defined for each intercompany organization when used as a provider, versus when used as a receiver in an intercompany transaction.

This can even be configured for individual users, where a user can be given different security grants for the same intercompany organization depending on whether the user acts as a provider or a receiver for an intercompany transaction.

Example

This example demonstrates how a user can have access to one intercompany organization but can have access to a different set of accounts depending on whether the user acts as a provider or a receiver for an intercompany transaction.

Let's look at the security grants of two users, Paul and Rita, who work for intercompany organizations IC-Org1 and IC-Org2 respectively.

- Paul manages intercompany transactions only for IC-Org1. He needs different account access as a provider and as a receiver.
- Rita manages intercompany transactions only for IC-Org2. She needs full access to all accounts for both provider and receiver business functions.

To achieve the access control for Paul, you assign rules that grant Paul access to different accounts as a provider and as a receiver.

User/Grant	Intercompany Data Access	Account Access	Business Function	Access level
Paul	IC-Org1	1100-1199	Provider Intercompany	Read and write

User/Grant	Intercompany Data Access	Account Access	Business Function	Access level
Paul	IC-Org1	2100-2199	Receiver Intercompany	Read and write

Note that no security grants are configured for Rita because she has access to all accounts, which is the default Segment Value Security by Business Function feature.

With the security grants that Paul carries, let us look at these scenarios:

Scenario 1: Paul in the role of a provider for a loan funding transaction. Here are the steps that Paul and Rita take to complete an intercompany transaction from IC-Org1 to IC-Org2.

- Paul creates an intercompany transaction for loan funding from provider IC-Org1 to receiver IC-Org2.
- Paul enters the provider distribution account. He can only select accounts from 1100 to 1199.
- Paul submits the loan funding intercompany transaction.
- Rita reviews the inbound transaction for IC-Org2 that Paul has initiated.
- Rita enters the receiver distribution account. She can select any account.
- Rita submits the intercompany transaction.

Scenario 2: Paul in the role of a receiver for an expense sharing transaction. Here are the steps that Rita and Paul take to complete an intercompany transaction from IC-Org2 to IC-Org1.

- Rita creates an intercompany transaction for expense sharing from provider IC-Org2 to receiver IC-Org1.
- Rita enters the provider distribution account. She can select any account.
- Rita submits the expense sharing intercompany transaction.
- Paul reviews the inbound transaction for IC-Org1 that Rita initiated.
- Paul enters the receiver distribution account. He can only select accounts from 2100 to 2199.
- Paul submits the intercompany transaction.

Important Notes

The Segment Value Security by Business Function feature has not been implemented for:

- Intercompany reports.
  - For example, users with limited access, who cannot view certain accounts on the intercompany UIs, will be able to see these accounts in the Intercompany Account Details report.
- Multitier Intercompany Operations module.
  - The security grants configured for intercompany does not apply to the Multitier Intercompany Operations feature.

Additional Notes

- The examples above demonstrate users with read/write access only. However, user access can be granted on a read/write or read-only basis to satisfy the business needs.
- Segment Value Security by Business Function applies to accounts that are generated by Transaction Account Builder (TAB). If the user creating the intercompany transactions does not have read/write access to the account, TAB will not generate the account.

- Segment Value Security by Business Function does not apply to application generated intercompany payables and receivables accounts. These accounts are generated accordingly regardless of how the Segment Value Security by Business Function is configured.
- Segment Value Security by Business Function applies to accounts generated along with intercompany transactions sourced from intercompany allocations. If the user executing intercompany allocations does not have read/write access to the account, intercompany allocations will fail to generate intercompany transactions.

Payables-Specific Considerations for Segment Value Security

Optimizing segment value security by business function limits a user's access to certain accounts for each secured value set while creating, updating, and reviewing financial data.

The security context of the business function enforces the segment value security. “Payables” is the applicable business function for Payables module. Payables users have the following access levels for the segment values of a secured chart of accounts based on the Payables business function:

- Read/write: This access level allows a user to manage invoice lines or distributions and inquire and review the invoice distributions with account values to which the user has read/write access.
- Read-Only: This access level allows a user to only view and inquire invoice distributions referencing those account values to which they've access. User can’t create transactions using these account values.

Note:

- This feature operates on the principle of first providing access to all the secured segment values to all users by default.
- Security policies are defined, and such rules are assigned to a user only when their access should be limited to specific segment values.
    - The user rule assignments are defined for a combination of business function, data access context, and access level. For Payables, the business function to use is “Payables” and the data access context is “Business Unit.”
    - If there are no matching rule assignments for a user for a given usage scenario, the user gets access to all account values for the secured chart of accounts value set.

Setting Up

There are no extra Payables-related setups to undertake to enable Segment Value Security by Business Function for Payables. However, to enforce segment value security in the Payables module, the “Payables” business function must be enabled for enforcement.

Enforcing Segment Value Security by Business Function in Payables

In Payables, the business unit serves as the data security-striping mechanism that controls the data access to the users, and also the security context basis for segment value security.

Whenever a Payables user accesses any of the Payables pages, the account combination values the user can access are decided by the intersection of data security access for the Payables module and the security context of the segment

value security for the Payables business function. For example, if user wants to create a Payables Invoice for Vision America business unit, then they should have the following access rights.

- Access to Vision America business unit in the Payables module
- Access to at least one account value in Vision America Payables business function in segment value security

Segment value security by business function can be enforced in the Payables modules differently based on the task pages you're working with.

Examples of Enforcing Segment Value Security While Creating or Processing Payables Invoices

Segment value security validation takes place on Create Invoice and Process Invoice pages even if the user just types in the account values instead of selecting them from the accounting key flexfield dialog box.

Here are a few examples scenarios of how Payables-specific segment value security is enforced.

Access to Account Segment Values

Users can enter an account combination on an invoice only if they've read/write access to each segment's account for the said account combination. Consider that User 1 has the following accesses.

- Read/write access to account values 5310 and 5320 in Vision America business unit.
- Read-only access to 7310 in Vision America business unit.
- Read/write access to account value 7320 in Vision Canada business unit.

User 1 can create an invoice for Vision America business unit with all account combinations that have account segment values of 5310 and 5320, but not account combinations with 7310 or any other account value. Similarly, User 1 can create an invoice for Vision Canada business unit with all account combinations that have account segment values of 7320 only, and not with any other account value.

Segment value security by business function is also enforced when the user creates invoices through the ADFDI spreadsheet, and through the import process. It's also enforced while entering the account combination details during the workflow process.

Note: Segment value security by business function isn't enforced when invoices are created from internal source, such as the following.

- Advance schedule billing notice
- Evaluated Receipt Settlement (ERS)
- Advanced Global Intercompany (AGIS)
- Sales Compensation
- Assets
- Projects
- One-Time Payments (OTP)
- Property Manager
- Patient refunds
- Projects intercompany invoices
- Projects interproject invoices
- Student Management
- Receivables
- Expenses (includes cash advances and expense reports)
- Return to supplier
- Supplier Chain Financial Flow Orchestration
- Fiscal Document Capture

Access to Accounts used in Distributions

Users can't cancel an invoice or invoice line or invoice distribution if the entity has at least one distribution with an account combination to which they don't have read/write access. What this means is that the user can only cancel an invoice or its lower entity if they've complete access to all the accounts used in its distributions.

Consider that User 2 has read/write access to account values 5310 and 5320 but read-only access to 7310. There are 2 invoices with following account details.

- Invoice 1: Has two distributions, one with account combination of 5310 and other with 5320.
- Invoice 2: Has two distributions, one with account combination of 5310 and other with 7310.

The user can cancel Invoice 1 because they've read/write access to both account segment values 5310 and 5320. However, user can't cancel Invoice 2 because they don't have read/write access to 7310.

Access to Account Combinations

When a user tries to validate an invoice with an account combination for which they don't have read/write access, the invoice is placed on hold, and distributions must be generated for the account combination. This means that the user can't trigger automatic distribution generation if they don't have read/write access to the account combination.

Consider that User 3 has read/write access to account values 5310 and 5320 and read-only access to 7310. There are two invoices with following account details.

- Invoice 1 has two invoice lines, one with account combination of 5310 and other with 5320.
- Invoice 2 has two invoice lines, one with account combination of 5310 and other with 7310.

The user can validate Invoice 1 because they've read/write access to both account segment values 5310 and 5320. However, they can't validate Invoice 2 because they've read/write access to only 5310 but not 7310.

Access to Accounts used in Prepayment Distributions

A user can't apply or unapply prepayments if the prepayment invoice distributions include an account value to which they don't have read/write access.

Consider that User 4 has read/write access to account values 6110 and 6120 and read-only access to 8110. There are two prepayment invoices with following account details.

- Invoice 1 has two prepayment distributions, one with account combination of 6110 and other with 6120.
- Invoice 2 has two prepayment distributions, one with account combination of 6110 and other with 8110.

The user can apply prepayment to Invoice 1 because they've read/write access to both account segment values 6110 and 6120. However, they can't apply or unapply the prepayment to invoice 2 because they don't have read/write access to 8110.

Examples of Enforcing Segment Value Security While Viewing Payables Invoice Lines

Segment value security isn't enforced on view invoice lines. Any user can view the invoice lines irrespective of their security access regarding segment value security.

However, segment value security is still enforced in the following scenarios.

Read Access to Invoice Distributions

When users navigate to the Distributions page of an invoice, they can see only the invoice distributions referencing the account values to which they've either read/write or read-only access. Other distributions aren't displayed. However,

if the users don't have any Payables-specific segment value security rule assignments, they can see all the distribution lines.

Consider that the user has read/write access to account value 5310, read-only access to 7310, and no access to 8310. The user navigates to the Distributions page for the following invoices.

- Invoice 1 has three invoice distributions where one distribution has account combination of 5310, the second one with account value of 7310, and the third with 8310. When user navigates to the Distributions page, they can see only the distribution lines with account values of 5310 and 7310. User can't see the distribution line with the account value of 8310 because they don't have read access to this value.
- Invoice 2 has three invoice distributions where one distribution has account combination of 5310, the second and third distribution lines have account combinations with the account value of 7310. When the user navigates to the Distributions page, they can see all three distributions as the user has read access to both 5310 and 7310.

Read Access to Accounting Combinations

When a user reviews the Transaction Accounting page, they can see only the accounting lines that have an account combination to which they've either read/write or read-only access. Other accounting lines aren't displayed. If the user doesn't have any specific rule assignments, then they can see all the distributions.

Consider that the user has read/write access to account value 5310, read-only access to 7310, and no access to 8310. The user navigates to the View Accounting page for the following invoices.

- Invoice 1 has three invoice distributions where one distribution has account combination of 5310, the second with account value of 7310, and third with 8310. When the user navigates to the View Accounting page, they can see only the accounting lines with the account values of 5310 and 7310. However, user can't see the accounting line with the account value of 8310 as they don't have read access to this value.
- Invoice 2 has three invoice distributions where one distribution has account combination of 5310, the second and third distribution have an account combination each with account value of 7310. When the user navigates to the View Accounting page, they can see all accounting lines as the user has read access to both 5310 and 7310.

Read Access to Account Values

When a user drills down to invoice distributions, say from Payments or from GL journal entries, they can see only the invoice distributions referencing account values to which they either have read/write or read-only access. Other distributions aren't displayed. If the user doesn't have any Payables-specific segment value security rule assignments, then they can see all the distributions.

Receivables-Specific Considerations for Segment Value Security

Chart of accounts segment value security controls user access to chart of accounts-based accounting information in Receivables.

Use segment value security to define user access to Accounting Flexfield segment values in Receivables. A given user can only work with account values in the secured chart of accounts value set to which they've been granted access and at the level of their rule assignments.

Segment value security doesn't affect Receivables setup or transaction creation.

Enable Receivables for Segment Value Security by Business Function

Use the Manage Segment Value Security by Business Function action in the Manage Chart of Accounts Configuration page to enable Receivables for segment value security.

To enable Receivables for segment value security:

1. Navigate to the Manage Chart of Accounts Configurations task.
2. In the Manage Chart of Accounts Configurations page, click the **Manage Segment Value Security by Business Function** button.
3. In the Manage Segment Value Security by Business Function window, enable the **Receivables** option.
4. Save your work.

When you enable segment value security for Receivables, by default all Receivables users are granted access to all segment values. You must set up rules to restrict user access to Accounting Flexfield segment values by business function. In the context of the Receivables business function, **business unit** is the security context.

Set Up Segment Value Security Rules in Receivables

Use the Manage Segment Value Security Rule Assignments spreadsheet to assign segment value security rules to the users who require some form of restricted access to Accounting Flexfield segment values.

As a general rule, create dedicated segment value security roles for each designated group of Receivables users and the related data security policies that govern their access to secured segment account values.

> **Note:** Never directly create segment value data security policies using the existing Receivables job roles, such as Receivables Manager. The existing job roles are likely to be shared by all Receivables users, and many separate groups of users are likely to have different chart of account segment value security profiles.

The dedicated segment value security roles you create, with their accompanying secured segment values, can be assigned to and even shared among the corresponding users based on their particular segment value access requirements.

You can enable security enforcement for all business functions or for one or more specific business functions. This table provides an example of how to designate segment value access rule assignments to Receivables users.

Segment Value Access

Access Type	Business Function	Security Context	Security Context Value
Global access	All business functions	All security contexts	All security context values
Access to Receivables business function only	Receivables	Business unit	All business units
Access to a specific business unit of Receivables business function	Receivables	Business unit	Name of the specific business unit

Global access: Assign global access to users with responsibilities across multiple business functions, for example, Assets, Receivables and General Ledger. Global access users would then require access to the same specified segment account values across all their assigned asset books (FA), business units (AR), and ledgers (GL).

Access for Receivables business function only: Assign business-function-only access to users with the Receivables responsibility who require access to the same specified segment account values for all their assigned business units.

Access for a specific business unit: Assign specific business unit access to users with the Receivables responsibility who require access to the specified segment account values for one business unit only.

Read-Write and Read-Only Access

You can further restrict user access to accounting flexfield segment values by assigning users Read-Write and Read-Only privileges.

- Read-Write: Users can create and update transactions, view accounting, and report on Receivables transactions that reference the account values granted.
- Read-Only: Users can view, query, and report on Receivables transactions that reference the account values granted. For example, users who don't have Read-Write access to segment values belonging to transaction distributions can still search for and review these distributions.

Summary of Segment Value Security Enforcement in Receivables

Users with Read-Write access to specified account values can take these actions on the transactions that reference these account values:

- Create, save and complete a transaction.
- Credit a transaction.
- Update account values in the distributions belonging to a transaction.
- Post transactions to General Ledger.
- Apply a receipt or credit memo to a transaction.
- Unapply a receipt or credit memo from a transaction.
- Manage adjustments to transactions.
- Create draft subledger accounting.
- Use these web service components: Get, Create, Update, Delete, Reverse.

Users with Read-Only access to specified account values can take these actions on the transactions that reference these account values:

- Create and save a transaction.
- View transaction distributions.
- Run reports.

Segment value security isn't enforced on these activities:

- Receivables implementation tasks in Functional Setup Manager.
- These reports in Scheduled Processes:
  - Receivables Aging by GL Account Report
  - MFAR Aging and Reconciliation Report
  - General Ledger Reconciliation Report

Example of Segment Value Security Enforcement in Receivables

The following example illustrates segment value security enforcement by business function in Receivables.

User Perry has the Accounts Receivables Manager role, but isn't assigned any segment value security rules. This implies that Perry has global access to all accounts.

User James, who also has the Accounts Receivables Manager role, has access to two business units: Vision ASC605 BU001 and Vision ASC605 BU002. The details of the access are described in the following table.

Example of Segment Value Security

User	Role	Business Function	Business Unit	Security Context Value (Cost Center) as per the rule assignments	Access Level
James	Accounts Receivable Manager	Receivables	Vision ASC605 BU001	00000000, 20000000 to 20000220	Read-Only
James	Accounts Receivable Manager	Receivables	Vision ASC605 BU002	00000110, 20000221 to 20000440, 30000550	Read-Write

This table describes the results of the various actions that James attempts on the Create Transaction: Invoice page in each business unit, as determined by James' segment value security assignments. The Cost Center Value column represents the cost centers used in the transaction.

User Actions and Results

User	Business Unit	Cost Center Value	Access Level	Action	Result
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Save Transaction	James can save the transaction.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Review Distributions	James can review distributions for which James has read-only access. James can't view the account of the distribution with cost center value 30000330.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Edit Distributions	James can't edit or even see the distribution segment values.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Complete Transaction	James can't complete the transaction.
James	Vision ASC605 BU001	00000000, 20000220, 30000330	Read-Only	Post to Ledger	James can't post the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Save Transaction	James can save the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Review Distributions	James can review all distributions.

User	Business Unit	Cost Center Value	Access Level	Action	Result
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Edit Distributions	James can edit distributions and change the cost center.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Complete Transaction	James can complete the transaction.
James	Vision ASC605 BU002	00000110, 20000440	Read-Write	Post to Ledger	James can post the transaction.

Subledger Accounting-Specific Considerations for Segment Value Security

This section explains the purpose of Segment Value Security by Business Function and provides an overview of Subledger Accounting, including its activities, setup, transaction processing, and how data security is applied.

Oracle Subledgers such as Payables, Receivables, and so on. and Fusion Accounting Hub subledgers are used to capture transaction information which is then processed by the Subledger Accounting engine to generate detailed subledger accounting entries.

In general, Subledger Accounting activities include:

- **Setup:** Configuring subledger applications, accounting options, accounting rules, mapping sets and supporting references.
- **Transaction:** Fusion Accounting Hub transaction import, create accounting and posting to the General Ledger, manual adjustment entry, maintaining control balances and supporting reference balances.
- **Inquiry and Reporting:** Review subledger accounting entries and drill down to source transactions, reviewing reports such as the Subledger Period Close Exception report, Account Analysis report, OTBI reporting on Subledger Accounting Entries and Supporting Reference balances, and so on.

Subledger Accounting doesn't deliver any job roles for Fusion Applications. Applications such as Payables. Receivables, and so on. which consume Subledger Accounting services grant access to accounting related activities for their application specific job roles by inheriting the duty roles provided by Subledger Accounting.

Accounting Hub users are required to define custom job roles and assign the appropriate duty roles as needed to perform accounting activities.

No data security is applied for the setup related activities; however, data security is applied on the Ledger and Journal Source LOVs for the Transaction, Inquiry and Reporting activities listed above. Data security is implemented through grants against the job roles which perform subledger transaction, inquiry and reporting activities. For example – Accounts Payable Supervisor requires access to account payables invoices, view accounting, review the subledger accounting entries created or create adjustment accounting entries for Payables journal source.

Here is a summary of how data security is applied on Subledger Accounting for General Ledger and Subledger Job Roles:

Job Role	Default Data Security
General Ledger Job Roles (General Accounting Manager, Financial Specialist, and so on.)	For the ledgers to which user has data access: • Review or create subledger accounting entries for ALL subledger applications. • Account transactions, transfer to general ledger and drill down to view transaction page for ALL subledger applications. • Inquiry and reporting pages for ALL subledger applications.
Oracle Subledger Job Roles (Payables Supervisor, Receivables Specialist, and so on.)	For the specific security context (i.e. Business Unit, Intercompany Organization, Asset Book, and so on.) to which user has data access: • Review or create subledger accounting entries for the subledger application. • Account transactions, transfer to general ledger and drill down to view transaction page for the subledger application. • Inquiry and reporting pages for the subledger application.

Segment Value Security by Business Function Implementation in Subledger Accounting

This topic outlines how Segment Value Security is implemented in Subledger Accounting and how it affects different setup, transaction, and reporting areas.

Subledger Accounting is an intermediate processing layer which converts the transaction information from different Oracle and Accounting Hub subledgers into accounting entries based on the accounting rules defined in the system. The Subledger Accounting user interfaces and reports do not enforce data security through a specific data security context such as Data Access Set or Business Unit. Data Security in Subledger Accounting is governed by the data security policies associated with the Job Role which has associated subledger functions.

Subledger Accounting doesn't have any associated business function. For some of the Subledger Accounting pages such as the ones associated with adjustment subledger accounting entry creation or review, the General Ledger business function context is applied. General Ledger enforces data security through Data Access Sets which control read and write access to the entire ledger, or just to certain primary balancing segment values. When the General Ledger business function is applied on subledger accounting pages, a cumulative effect of all the Data Access Set grants for the user will be applied since subledger accounting pages do not have a Data Access Set context. They provide access for the associated ledger only.

If the subledger accounting entries are viewed in the context of a transaction for Oracle Subledgers such as View Accounting window, the business function of the associated subledger shall be applied.

If the segment value security policies are defined for All business functions, access to the secured segment values is based on the applicable Security Context is applied. For example, if the Security Context is set to Data Access Set, subledger accounting pages which enforce General Ledger business function (Create Subledger Journal, Review Subledger Journals, and so on.) will restrict access to the corresponding secured segment values on these pages. However, in the View Accounting page which applies the Subledger business function, these values would not be accessible to users.

If the segment value security policies are defined for All business functions and All security contexts, then access will be restricted to the corresponding secured segment values in all subledger accounting pages where Segment Value Security by Business Function is enforced.

Here is a summary of how Subledger Accounting implements Segment Value Security by Business Function in the different Setup, Transaction and Reporting areas where chart of accounts segments is involved –

Area	User Interface	Segment Value Security by Business Function	Business Function Context Applied
Setup	All Setup Pages	Not Applied	Not Applicable
Transaction	Create Manual Subledger Journal using UI or Spreadsheet	Applied	General Ledger
	Create Accounting Online / Batch process	Not Applied	Not Applicable
	Create Accrual Reversal Accounting process	Not Applied	Not Applicable
	Create Multiperiod Accounting process	Not Applied	Not Applicable
	Update Subledger Balances process	Not Applied	Not Applicable
	Import Accounting Transactions	Not Applied	Not Applicable
Inquiry and Reporting	Review / View Subledger Journal	Applied	General Ledger
	Review / View Subledger Journal – Account Override	Applied	General Ledger
	View Accounting	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	View Accounting – Account Override	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	Drill Down – Subledger Journal Lines	Applied	General Ledger
	Drill Down – View Transaction	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	T-Account Report – Review Subledger Journals	Applied	General Ledger
	T-Account Report – View Accounting	Applied	Subledger Context is applied for the supported subledgers (For example: Payables, Receivables, and so on.)
	Journal Entries Report	Applied	General Ledger
	Account Analysis Report	Applied	General Ledger
	Create Accounting Execution Report	Applied	General Ledger
	Create Multiperiod Accounting Execution Report	Applied	General Ledger

Area	User Interface	Segment Value Security by Business Function	Business Function Context Applied
	Create Accrual Reversal Accounting Execution Report	Applied	General Ledger
	Subledger Accounting Methods Setup Report	Not Applied	Not Applicable
	Accounting Event Diagnostics Report	Not Applied	Not Applicable
	Third Party Control Account Balances Report	Not Applied	Not Applicable

Case Study: Application of Segment Value Security

Joe and Cassie are employees of the Vision Corporation organization.

Vision Operations business unit is one of many business units under the **Vision Corporation US** ledger which manages the Payables and Payment business functions specifically. To streamline access for accounting users based on balancing segment values, the **Vision Corporation US** ledger has 3 Data Access Sets defined – **Vision Corp DAS A**, **Vision Corp DAS B** and **Vision Corp DAS C**, other than the implicit DAS **Vision Corporation US**.

Joe has been hired as a Payables Specialist of Vision Operations in the US to manage payables invoicing related activities such as verifying and recording supplier invoices in the system, making payments timely, monitoring expenses, and keeping a track of all the documents for tax purposes. In certain cases, Joe may be required to enter subledger adjustment accounting entries if the invoice was not captured directly in the Payables – Invoices application.

Cassie has been hired as a General Accountant of Vision Corporation in the US for reviewing account statements, conducting data analysis with financial transactions, and generating reports on revenues, expenses, asset, liability, and equity accounts. She is also responsible for recording accounting adjustments, accruals, allocations, currency revaluations and translations as part of accounting period closure activities. Occasionally, she may create subledger adjustment accounting entries during subledger to general ledger reconciliation.

The following are the job roles and data security assignments provided to Joe and Cassie for managing the responsibilities related to Payables Specialist and General Accountant job roles –

User	Job Role	Data Security Context
Joe	Employee	NA
	Payables Specialist	Vision Operations (BU)
Cassie	Employee	NA
	General Accountant	Vision Corp DAS A
	General Accountant	Vision Corp DAS C

Subledger Accounting doesn't have any separate data security context or business function. By default, all segment values corresponding to the secured segments in the account combination are accessible to perform the activities which are accessible to the Payables Specialist and General Accountant job roles on the Vision Operations business unit and Vision Corporation US ledger respectively. Access to specific segment values of the secured segments while entering an account combination in Payables and General Ledger pages would be restricted based on the respective policies assigned to each user.

Following segment value security policies are assigned to Joe and Cassie –

User	Job Role	Data Security Context	Business Function	Segment	Segment Value	Access Level
Joe	Employee	NA	NA	NA	NA	NA
	Payables Specialist	Vision Operations (BU)	Payables	Cost Center	110	Read/Write
					120	Read Only
	Payables Specialist	Vision Corporation US (DAS)	General Ledger		130	Read/Write
Cassie	Employee	NA	NA	NA	NA	NA
	General Accountant	Vision Corp DAS A (DAS)	General Ledger	Cost Center	110	Read/Write
					120	Read/Write
					130	Read Only
					140	Read Only
		Vision Corp DAS C (DAS)			160	Read/Write
					170	Read/Write

Here are some sample examples of how the above policy definition would provide access to different subledger accounting pages to Joe and Cassie respectively –

User	User Interface	Access
Joe	View Accounting	This page is read-only, and the Subledger business function is applied here. Since the user has access to read both the cost center values 110 and 120 for Payables business function, they will be able to access those account combinations which use these cost center values.
	View Accounting – Account Override	This page supports read\write and the Subledger business function is applied here. Since the user has access to read\write to the cost center value 110 only, they will be able to access those account combinations which use this cost center value.
	Review Journal Entries / Journal Lines	This page is read-only, and the General Ledger business function is applied here. Since the user has access to read the cost center value 130 for General Ledger business function, they will be able to access those account combinations which use this cost center value.
	Account Analysis Report	This is a read-only report, and the General Ledger business function is applied here. Since the user has access to read the cost center value 130 for General Ledger business function,

User	User Interface	Access
		they will be able to access those account combinations which use this cost center value.
	Create Subledger Journal	This page supports read\write and the General Ledger business function is applied here. Since the user has access to read\write the cost center value 130 only, they will be able to access those account combinations which use this cost center value.
Cassie	Review Journal Entries / Journal Lines	This page is read-only, and the General Ledger business function is applied here. The user has access to read the cost center values 110, 120, 130, 140 through the data access set **Vision Corp DAS A** and the cost center values 160, 170 through the data access set **Vision Corp DAS C**. So, a cumulative effect of all the Data Access Set grants will be applied for the General Ledger business function here, thereby allowing the user to access those account combinations which use the cost center values – 110, 120, 130, 140, 160 and 170.
	Account Analysis Report	This is a read-only report, and the General Ledger business function is applied here. Like the above scenario, a cumulative effect of all the Data Access Set grants will be applied for the General Ledger business function here, thereby allowing the user to access those account combinations which use the cost center values – 110, 120, 130, 140, 160 and 170.
	Create Subledger Journal	This page supports read\write and the General Ledger business function is applied here. The user has access to read\write the cost center values 110, 120 through the data access set **Vision Corp DAS A** and the cost center values 160, 170 through the data access set **Vision Corp DAS C**. As a cumulative effect of all the Data Access Set grants applied for the General Ledger business function here, the user gets access to those account combinations which use the cost center values – 110, 120, 160 and 170.

How You Segregate Import Journals Access from FBDI Import for Journals Access

You can restrict the combined use of the Import Journals process and the Load Interface File for Import process for file-based data import (FBDI) journals to certain users.

Users who aren't authorized to import journals using FBDI can be assigned privileges that allow them to submit journal import only for processes such as Create Accounting for subledger transactions and Oracle General Ledger journal creation through the Application Development Framework desktop integration (ADFdi) spreadsheet.

Separate privileges give you the flexibility to assign different users different levels of access to the Import Journals process to optimize security control and prevent interruptions in FBDI journal import procedures that are reserved for automated and mass volume imports.

Here are the privileges that allow access to journal import processes other than FBDI import for journals.

- **Run Import Journals Program without FBDI Access** (GL_RUN_IMPORT_JOURNALS_PROGRAM_WITHOUT_FBDI_ACCESS): Allows submission of the journal import program using the Oracle Fusion Enterprise Scheduler Services. However, this privilege does not include the ability to use the Import Journals process when submitting the Load Interface File for Import program to support creating journal records using File Based Data Import.
- **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** (XLA_POST_SUBLEDGER_JOURNAL_ENTRY_TO_GL_NO_JOURNAL_IMPORT_ACCESS_FOR_FBDI): Allows submission of the program to transfer to and post journal entries in General Ledger. However, this privilege does not include the ability to use the Import Journals process when submitting the Load Interface File for Import program to support creating journal records using File Based Data Import.

These privileges aren't assigned to any predefined role. You must assign them to a custom role to use them as substitutes for the **Run Import Journals Program** (GL_RUN_IMPORT_JOURNALS_PROGRAM_PRIV) and **Post Subledger Journal Entry to General Ledger** (XLA_POST_SUBLEDGER_JOURNAL_ENTRY_TO_GENERAL_LEDGER_PRIV) privileges, which allow access to FBDI import for journals.

If you're creating a role based on the predefined General Accountant job role, here's a summary of the steps you would follow to prevent a user from using FBDI journal import, while still allowing that user to submit journal import through other processes.

1. Use the Security Console to make a deep copy of the predefined General Accountant job role by copying its top role and inherited roles. The inherited roles include the Journal Management and Subledger Accounting Manager duty roles.
2. After the role has been copied, search for the Journal Management custom duty rule that was generated. Perform the following actions in the Function Security Policies step:
    a. Add the **Run Import Journals Program without FBDI Access** privilege.
    b. Delete the **Run Import Journals Program** privilege.
3. Search for the Subledger Accounting Manager custom duty role that was generated. Perform the following actions in the Function Security Policies step:
    a. Add the **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privilege.
    b. Delete the **Post Subledger Journal Entry to General Ledger** privilege.

If you're creating your own custom role or starting with an existing custom role, perform these steps in the Security Console to prevent a user from using FBDI journal import, while still allowing that user to submit journal import through other processes.

1. Add the **Run Import Journals Program without FBDI Access** and **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privileges.
2. Delete the **Run Import Journals Program** and **Post Subledger Journal Entry to General Ledger** privileges wherever they exist in the role hierarchy.

Note: Users who already submit the Load Interface File for Import for other import processes such as Import Bank Statements from a Spreadsheet and Import AutoInvoice won't be impacted by the removal of the **Run Import Journals Program** and **Post Subledger Journal Entry to General Ledger** privileges.

If a user who's only assigned the **Run Import Journals Program without FBDI Access** or the **Post Subledger Journal Entry to General Ledger No Journal Import Access for FBDI** privilege submits the Load Interface File for Import process for the Import Journals process, the job will end in error. The log file will display an insufficient permissions message.

Related Topics

- Create ERP Roles in the Security Console
- Guidelines for Copying ERP Roles

FAQs for General Ledger

What happens when changes are made to an account hierarchy that's referenced in segment value security rules?

The tree is set from an active to a draft state when it's updated. The rules referencing the account hierarchy become ineffective.

After making changes to your hierarchy, you can submit the Process Account Hierarchies process to automatically run the required steps for processing account hierarchies updates in one submission, including:

- Tree audit
- Tree activation
- Row flattening
- Column flattening
- Maintain value set
- Maintain account hierarchy
- Publish hierarchy

With a successful audit process, the hierarchy is set back to an active status. The rules referencing the account hierarchy go back to being effective using the updated hierarchy.

Run the row and column flattening processes for the updated hierarchy as the flexfield component in the application as well as other hierarchy processes rely on the flattened hierarchy data to come up with the list of values available to the user to properly secure the correct account values.

Run the Maintain Value Sets and Maintain Chart of Account Hierarchies processes, particularly for hierarchy changes to the primary balancing segment value set if such values are referenced in your primary balancing segment value based data access sets. These processes update the data that is required to regulate ledger and data access security by storing:

- Primary balancing segment values assigned to a ledger.
- Specific child balancing segment values assigned to a data access set through parent value assignments.

Note: If you change an account hierarchy that's already published and you inquire or report on summary balances based on this changed hierarchy, you must republish to reflect the updated hierarchy in the balances cube.

When does security take effect on chart of accounts value sets for balances cubes?

To enforce segment value security according to defined security policies, you must publish an account hierarchy to the balances cube after enabling security for its value set.

If you disable security for that value set, you must likewise publish its account hierarchy to the balances cube to register that security is no longer enabled for it.

Once segment value security is enforced, you don't have to republish account hierarchies if you define new security policies or modify existing policies for the secured value set, even if the security definition has hierarchical conditions that use parent values.

How can I secure the data in GL balances cubes?

Use data access set and segment value security to secure dimension values such as ledger and chart of account values.

For chart of accounts dimension values, security restricts the display of data associated with the secured values, but not the selection of the values themselves. For example, when submitting a report, you can select company value 100 in your report definition when selecting the Point of View, even if you weren't granted access to that company value. However, you can't see the data associated with company 100 in your report.

Payables

Payables Security

Oracle Fusion Payables improves security by limiting access to invoices and payments by business unit. You can access invoices and payments for viewing or processing only for the business units to which you've permission. The permission must be explicitly granted to each user.

Assign users to the appropriate security context, such as a business unit, for job roles from the Manage Data Access for Users page.

Oracle Payables is integrated to the document repository for processing scanned invoices. To edit any invoices in the repository, you can create a custom role with the Edit Payables Invoice (AP_EDIT_PAYABLES_INVOICE_PRIV) or Create Payables Invoice (AP_CREATE_PAYABLES_INVOICE_PRIV) privileges.

Keeping up with the security requirements, the following predefined roles have view-only access to the document repository:

- Financial Application Administrator
- Cost Accountant
- Project Accountant

Note: For further information, see the chapter Role Configuration Using the Security Console in the Securing ERP guide.

Why do I see a blank page on clicking View Invoice from Approval Notification?

A user must have these privileges to view an invoice by clicking the View Invoice button on the notification.

- View Payables Invoice
- Manage Payables Invoices
- Manage Payables Invoices Activities

If you've a custom user role, you might be missing these privileges, which results in the blank page being displayed.

Subledger Accounting

Security for Subledger Accounting

Oracle Fusion Subledger Accounting features require both function and data security privileges.

Overview

Security for Subledger Accounting includes:

- Setup task security
    - Security to configure accounting rules to define accounting treatments for transactions.
- Transaction task security
    - Security to create subledger journal entries (manual subledger journal entries or those generated by the Create Accounting process or Online Accounting).
    - Security to review and generate reports of subledger journal entries and lines.

Security to Perform Setup Tasks

Use the Define Subledger Accounting Rules task in the Setup and Maintenance work area to configure subledger accounting rules.

To configure subledger accounting rules, the setup user must be provisioned with a role that includes the Subledger Accounting Administration duty role.

- In the security reference implementation, the Financial Application Administrator job role hierarchy includes the Subledger Accounting Administration duty role. This role provides the access to configure your accounting rules.
- For more information about available setup job roles, duty roles and privileges, see the Oracle Financial Security Reference Manual.

Security to Perform Transactional Tasks

To create and view subledger journal entries, you must have the necessary access to perform the tasks in the relevant subledger work areas. Predefined subledger job roles include the entitlement to create and view subledger journal entries for subledger transactions you are authorized to access.

Security for Accounting Transformations in Accounting Hub

Accounting transformations require both function and data security privileges.

Oracle Accounting Hub security for accounting transformations includes:

- Setup task security
  - Security to register source systems into Accounting Hub.
  - Security to configure accounting rules to define accounting treatments for transactions.
- Transactional task security
  - Security to create subledger journal entries (manual subledger journal entries or those generated by the Create Accounting process).
  - Security to review and generate reports of subledger journal entry headers and lines.

Security to Perform Setup Tasks

Use the Define Accounting Transformation Configuration task in the Setup and Maintenance work area to integrate your external source system with the Accounting Hub.

To register your external source system and configure accounting rules, the setup user must be provisioned with a role that includes the following duty roles:

- Application Implementation Consultant
- Accounting Hub Integration
- In the security reference implementation, the Financial Application Administrator job role hierarchy includes the Accounting Hub Administration Duty role. This role provides the access to integrate your external source systems with accounting transformations.

Security to Perform Transactional Tasks

To import transaction data for accounting and posting in general ledger, the user must be provisioned with a job role that is associated with the Accounting Hub Integration duty role.

- The Import Subledger Accounting Transactions (XLA_IMPORT_SUBLEDGER_ACCOUNTING_TRANSACTIONS_PRIV) privilege is assigned to the Accounting Hub Integration duty role. This role enables the user to submit the Import Subledger Accounting Transactions process. This process also creates accounting entries and posts them in the general ledger.

To create and view subledger journal entries as an independent task, you must have the access necessary to perform the tasks. These tasks can be opened from the Oracle General Ledger, Journals work area. You must have access to the work area, as well as all of the ledgers (primary, secondary and reporting currency) in which the journal entry is posted.

The following are defined in the security reference implementation:

- The General Accounting Manager job role hierarchy includes duty roles that provide the entitlement to manage general accounting functions. This entitlement provides access to the general ledger, Journals work area.

The following duty role must be assigned directly to the General Accounting Manager job role to provide access to create and view subledger journal entries:

- Accounting Hub Integration Duty

Alternatively, you can assign the Subledger Accounting Duty and Subledger Accounting Reporting Duty roles to any of the following general ledger job roles:

- Chief Financial Officer
- Controller
- Financial Analyst
- General Accountant

For more information about available setup job roles, duty roles, and privileges, see the Oracle Financials Cloud Security Reference guide on the Oracle Help Center.

Related Topics

- Data Security

Cash Management

Considerations When You Create Accounts

Banks, branches and accounts fit together on the premise of the Bank Account model. The Bank Account model enables you to define and track all bank accounts in one place.

The Bank Account Model can explicitly grant account access to multiple business units, functions, and users. Consider the following when you set up bank accounts:

- Assign a unique general ledger cash account to each account, and use it to record all cash transactions for the account. This facilitates book to bank reconciliation.
- Grant bank account security. Bank account security consists of bank account use security, bank account access security, and user and role security.

Legal Entity-Based Data Access for Bank Account Setup

By default, users with the necessary function security privileges have access to create and manage all internal bank accounts.

Optionally, restrict access to bank account information based on the user's legal entity data access. This allows cash managers to add, review, or modify only the bank accounts associated with the legal entities that the user has access to. For example, only users who have been assigned the Manage Bank Account (CE_MANAGE_BANK_ACCOUNT_PRIV)

privilege for Vision Operations legal entity, can create, review, or modify internal bank accounts associated with this legal entity.

Decentralized organizations will benefit with improved security by ensuring that users only manage the bank account setup for the organizations they're authorized for.

Business benefits include:

- Improve security and increase control of bank account setup by limiting user access to bank account information.
- Helps decentralized organizations that require users only to manage the bank account information for the organizations they're authorized for.

To enable the feature Legal Entity-Based Data Access for Bank Account Setup, you must:

1. Use the Opt in UI to enable the feature.
2. Assign users to the appropriate legal entity security context:
    a. In the Setup and Maintenance work area, Select the Offering as Financials, Functional Area as Users and Security, and Task as Manage Data Access for Users.
    b. On the Manage Data Access for Users page, create data access for users by entering the user name, Cash Manager as role, legal entity as security context, and legal entity name as security context value, to create the data access for the user.
    c. Save the changes.

Once the feature is enabled, legal entity-based data access security is applied when an internal bank account is created or managed using either the UI or REST API.

Account Use

Account Use refers to accounts created for:

- Oracle Fusion Payables
- Oracle Fusion Receivables
- Oracle Fusion Payroll

Select the appropriate use or uses when creating an account in one or more of these applications.

Account Access

Payables and Receivables account access is secured by business unit. Before the bank account is ready for use by Payables or Receivables, you must:

1. Select the appropriate use for the application.
2. Grant access to one or more business units.

> **Note:** You can only assign access to the business units that use the same ledger as the bank accounts owning the legal entity,

User and Role Security

You can further secure the bank account so that it can only be used by certain users and roles. The default value for secure bank account by users and roles is No. For Payables and Receivables, you must have the proper business unit

assigned to access a bank account even if the secure bank account by users and roles is No. If the secure bank account by users and roles is set to Yes, you must be named or carry a role assigned to the bank account to use it.

- To set up banks, branches, and accounts, your custom role must have the security duty role Cash Management Administration. You must have the assigned the Manage Bank Account Security privilege (CE_MANAGE_BANK_ACCOUNT_SECURITY_PRIV) to modify the User and Role Security.
- To restrict the access to the Security tab, you must create a custom role and remove the Manage Bank Account Security (CE_MANAGE_BANK_ACCOUNT_SECURITY_PRIV) privilege. For example, you'd copy the Cash Management Administration duty role, rename it, and remove the privilege.

GL Cash Account Segments

Consider selecting the option to enable multiple cash account combinations for reconciliation to reconcile journal lines of multiple cash account combinations matching the same natural account and other specified segment values.

For example, if you set up 01-000-1110-0000-000 as your cash account, and select Account and Subaccount as GL Cash Account Segments, you can manually or automatically reconcile journal lines entered on different account code combinations matching the same natural account '1110' and subaccount '0000'.

Related Topics

- Assign Data Access to Users

Assets

Assets Data Security Components

In Oracle Fusion Assets, you can secure access to assets to perform transactions and view their information by asset book.

Every asset book created in Assets is automatically secured. You can perform transactions or view asset data only in the books to which you have permission. The permission must be explicitly granted to each user based on his or her duty requirements.

Data Privileges

Each activity is individually secured by a unique data privilege. In other words, when you provide access to a book, you actually provide permission to perform a particular activity in that book. For example, you can allow user X to perform only tasks related to asset additions in book AB CORP and restrict the same user from performing asset retirements in this book.

The data accesses for different asset activities are secured for the book with the following data privileges:

- Add Fixed Asset Data
- Change Fixed Asset Data
- Retire Fixed Asset Data
- Track Fixed Asset Data
- Submit Fixed Assets Reports

Asset Book Security Context

After you have completed your Assets setup, you can assign job roles to users using the Security Console and then grant explicit data access for asset books using the Manage Data Access for Users task from the Setup and Maintenance work area.

Default Asset Books

Since the data access is secured by book, you must provide or select the book to perform transactions and view asset details. If you have access to only one book, you can set up this book as the default book. The default book value must be set using the Default Book profile option. You set the value at the site, product, or user level. Usually, the default book is automatically entered in the Book field when you perform transactions and run reports. You can override the default value and enter another value from the list of values.

Related Topics

- Assets Profile Options

Payments

Options for System Security

Implement application security options on the Manage System Security Options page. You can set the application security to align with your company's security policy.

You can set security options for encryption and tokenization of credit cards and bank accounts, as well as for masking the payment instrument. Both funds capture and disbursement processes use security options.

> **Note:** You must enable encryption or tokenization of credit cards in Payments before you can import credit cards into Expenses.

Ask yourself these security questions to improve the security of your sensitive data:

- Which security practices do I want to employ?
- Do I want to tokenize my credit card data?
- Do I want to encrypt my bank account data?
- Do I want to encrypt my credit card data?
- How frequently do I want to rotate the master encryption key and the subkeys?
- Do I want to mask credit card and bank account numbers? How do I accomplish that?

To set up application security options, go to **Financials** > **Payments** > **Manage System Security Options** in the Setup and Maintenance work area.

Best Security Practices

These actions are considered best security practices for payment processing:

- Comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is the security standard required for processing most types of credit cards.
    - Comply with all requirements for accepting credit card payments.
    - Minimize the risk of exposing sensitive customer data.
- Create the master encryption key.
    - Rotate the master encryption key periodically.

Implementation Process of Master Encryption Key and Encryption

Before you can enable encryption for credit card or bank account data, you must automatically create a master encryption key. Oracle Platform Security Services stores your master encryption key. The application uses your master encryption key to encrypt your sensitive data.

Automatic creation of the master encryption key ensures that it's created and stored in the proper location and with all necessary permissions.

Credit Card Tokenization

If you tokenize your credit card data, you're complying with PCI DSS requirements. PCI DSS requires companies to use payment applications that are PCI DSS compliant.

Tokenization is the process of replacing sensitive data, such as credit card data, with a unique number, or token, that isn't considered sensitive. The process uses a third-party payment system that stores the sensitive information and generates tokens to replace sensitive data in the applications and database fields. Unlike encryption, tokens can't be mathematically reversed to derive the actual credit card number.

Click **Edit Tokenization Payment System** on the Manage System Security Options page to set up your tokenization payment system. Then, click **Tokenize** in the Credit Card Data section to activate tokenization for credit card data.

Credit Card Data Encryption

You can encrypt your credit card data to assist with your compliance of cardholder data protection requirements with these initiatives:

- Payment Card Industry Data Security Standard
- Visa's Cardholder Information Security Program

Credit card numbers entered in Oracle Receivables and Oracle Collections are automatically encrypted. Encryption is based on the credit card encryption setting you specify on the Manage System Security Options page.

> **Note:** If you import card numbers into Payments, you should run the Encrypt Credit Card Data program immediately afterward.

Bank Account Data Encryption

You can encrypt your supplier and customer bank account numbers.

Bank account encryption doesn't affect internal bank account numbers. Internal bank accounts are set up in Cash Management. They are used as disbursement bank accounts in Payables and as remit-to bank accounts in Receivables.

Supplier, customer, and employee bank account numbers entered in Oracle applications are automatically encrypted. Encryption is based on the bank account encryption setting you specify on the Manage System Security Options page.

> **Note:** If you import bank account numbers into Payments, you should run the Encrypt Bank Account Data program immediately afterward.

Master Encryption Key and Subkey Rotation

For payment instrument encryption, Payments uses a chain key approach. The chain key approach is used for data security where A encrypts B and B encrypts C. In Payments, the master encryption key encrypts the subkeys and the subkeys encrypt the payment instrument data. This approach enables easier rotation of the master encryption key.

The master encryption key is stored on Oracle Platform Security Services. Oracle Platform Security Services stores data in an encrypted format. The master encryption key can be rotated, or generated, which also encrypts subkeys, but doesn't result in encrypting the bank account numbers again.

If your installation has an existing master encryption key, click **Rotate** to automatically generate a new one.

> **Note:** To secure your payment instrument data, you should rotate the master encryption key annually or according to your company's security policy.

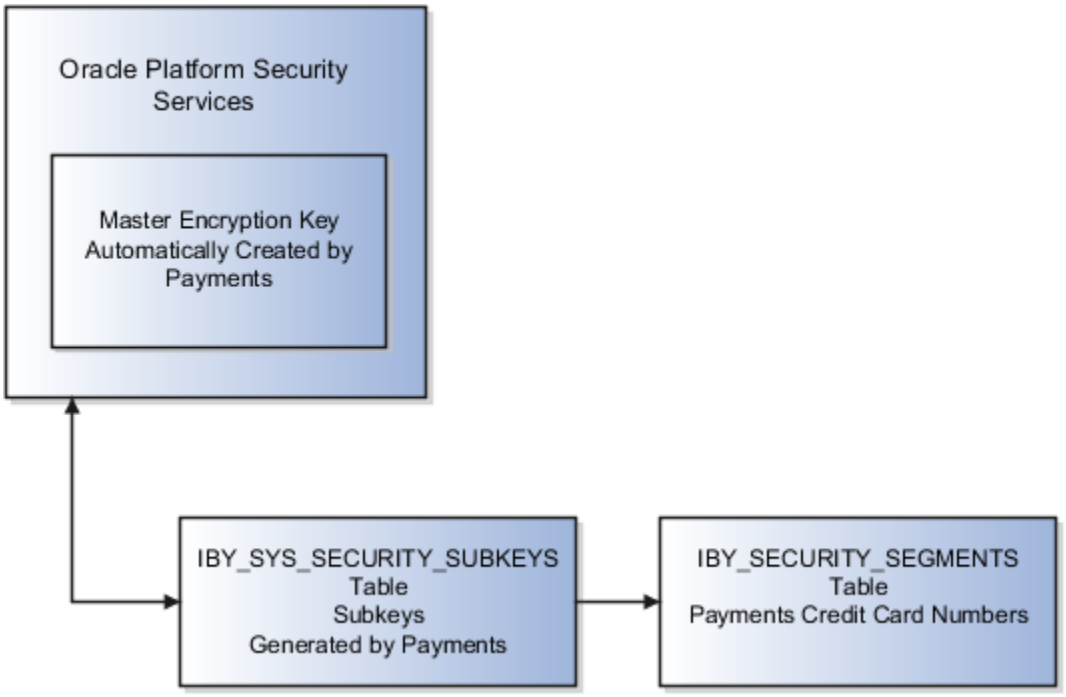
You can also select the frequency with which new subkeys are automatically generated, based on usage or on the maximum number of days. To specify a subkey rotation policy, click **Edit Subkey Rotation Policy**.

> **Note:** To secure your payment instrument data, you're advised to schedule regular rotation of the subkeys.

The security architecture for credit card data and bank account data encryption is composed of these components:

- Oracle Platform Security Services
- Payments master encryption key
- Payments subkeys
- Sensitive data encryption and storage

This figure illustrates the security architecture of the Oracle Platform Security Services repository, the master encryption key, and the subkeys.



Credit Card and Bank Account Number Masking

Payments serves as a payment data repository for customer and supplier information. It stores all of the customer and supplier payment information and their payment instruments, such as credit cards and bank accounts. It provides data security by letting you mask bank account numbers.

On the Manage System Security Options page, you can mask credit card numbers and external bank account numbers. You just have to select the number of digits to mask and display. For example, a bank account number of XX558012 displays the last six digits and masks all the rest. These settings specify masking for payment instrument numbers in the user interfaces of multiple applications.

> **Note:** For credit cards, you can unmask only up to the first or last four digits of the credit card number. On the other hand, you can unmask up to the first or last six digits of a bank account number.

Related Topics

- Enable Encryption of Sensitive Payment Information
- PCI DSS Credit Card Processing Requirements

Enable Encryption of Sensitive Payment Information

Financial transactions contain sensitive information, which must be protected by a secure, encrypted mode. To protect your credit card and external bank account information, you can enable encryption.

Encryption encodes sensitive data, so it can't be read or copied. To enable encryption, you must create a master encryption key. Oracle Platform Security Services is a repository that stores your master encryption key. The application uses your master encryption key to encrypt your sensitive data.

Note: Before you can import credit cards into Expenses, you must enable encryption or tokenization of credit cards in Payments. If you're using credit card data anywhere other than Expenses, you must enable tokenization in Payments.

To secure your credit card or bank account data, complete these steps:

1. In the Setup and Maintenance work area, go to **Financials** > **Payments** > **Manage System Security Options**.
2. On the Manage System Security Options page, click **Apply Quick Defaults**.
3. Select all the check boxes:
    - **Automatically create wallet file and master encryption key**
    - **Encrypt credit card data**
    - **Encrypt bank account data**
4. Click **Save and Close**.

Business Intelligence

Overview of Financial Reporting Security

Security for financial reporting uses Role Based Access Control, which has the following components:

- Users with roles.
- Roles that grant access to functions and data.
- Functions and data access that is determined by the combination of role.

Note: Users can have any number of roles.

Data security, which controls what action can be taken against which data, can also be applied to financial reporting. Data security is managed using:

- Data Access Sets:
    - Are defined to grant access to a ledger, ledger set, or specific primary balancing segment values associated with a ledger.
    - Permit viewing of journals, balances, and reports.
- Segment Value Security Rules:
    - Are set up on value sets to control access to parent or detail segment value for chart of accounts segments.
    - Restrict data entry, online inquiry, and reporting.

Note: For more information about security, see the Securing Oracle ERP Cloud guide.

Related Topics

- Overview of Data Access Set Security
- Examples of Data Access Set Security
- Overview of Segment Value Security
- Enforcement of Segment Value Security by Business Function

Oracle Fusion Transactional Business Intelligence Security

Oracle Fusion Transactional Business Intelligence is a real-time, self-service reporting solution.

All application users with appropriate roles can use Transactional Business Intelligence to create analyses that support decision making. In addition, business users can perform current-state analysis of their business applications using a variety of tools. These include Oracle Transactional Business Intelligence as the standard query and reporting tool, Oracle Analytics Answers, and Oracle Business Intelligence Dashboard tools. This topic summarizes how access is secured to Transactional Business Intelligence subject areas, Business Intelligence Catalog folders, and Business Intelligence reports.

Subject Areas

Subject areas are functionally secured using duty roles. The names of duty roles that grant access to subject areas include the words **Transaction Analysis Duty** (for example, **Payables Invoice Transaction Analysis Duty**).

The following table identifies the subject areas that predefined Financials job roles can access.

Financials Job Role	Subject Areas
Accounts Payable Manager	All Payables
Accounts Payable Specialist	All Payables
Accounts Payable Supervisor	Payables Invoices - Installments Real Time, Payables Payments - Disbursements Real Time, Payables Payments - Payment History Real Time
Accounts Receivable Manager	All Receivables
Accounts Receivable Specialist	All Receivables
Asset Accountant	Fixed Assets - Asset Depreciation Real Time, Fixed Assets - Asset Retirements and Reinstatements Real Time, Fixed Assets - Asset Source Lines Real Time, Fixed Assets - Asset Transactions Real Time, Fixed Assets - Asset Transfer Real Time
Asset Accounting Manager	All Fixed Assets
Budget Manager	Budgetary Control - Transactions Real Time

Financials Job Role	Subject Areas
Cash Manager	All Cash Management
Expense Manager	All Expenses
Financial Analyst	All Financials
Financial Application Administrator	All Financials
Financial Integration Specialist	All Financials
General Accountant	General Ledger - Journals Real Time, General Ledger - Period Status Real Time
General Accounting Manager	All General Ledger, All Payables, All Receivables
Intercompany Accountant	Financials Common Module - Intercompany Transactions Real Time
Tax Accountant	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time
Tax Administrator	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time
Tax Manager	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time, Receivables - Customer Tax Profile Real Time
Tax Specialist	Payables Invoices - Withholding Real Time, Receivables - Customer Account Site Tax Profile Real Time, Receivables - Customer Tax Profile Real Time

In addition, Oracle Fusion Cloud Financials includes predefined self-service reporting duties that provide access to Transactional Business Intelligence subject areas and drill down pages. They can be used as building blocks to construct reporting roles to provide self service reporting access.

This table identifies the subject areas that predefined Financials self-service reporting duty roles can access.

Financials Self-Service Reporting Duties	Subject Areas
Budgetary Control Self Service Reporting Duty	All Budgetary Control
Cash Management Self Service Reporting Duty	All Cash Management
Expense Self Service Reporting Duty	All Expenses
Fixed Asset Self Service Reporting Duty	All Fixed Assets
General Ledger Self Service Reporting Duty	All General Ledger, Financials Common Module - Intercompany Transactions Real Time

Financials Self-Service Reporting Duties	Subject Areas
Payables Self Service Reporting Duty	All Payables
Receivables Self Service Reporting Duty	All Receivables
Revenue Management Self Service Reporting Duty	All Revenue Management

Analyses fail if the user can't access all subject areas in a report.

Business Intelligence Catalog Folders

Business Intelligence Catalog folders are functionally secured using the same duty roles that secure access to the subject areas.

The following table identifies the folders that predefined Financials job roles can access.

Financials Job Role	Business Intelligence Catalog Folders
Accounts Payable Manager	Transactional Business Intelligence Payables
Accounts Payable Specialist	Transactional Business Intelligence Payables
Accounts Payable Supervisor	Transactional Business Intelligence Payables
Accounts Receivable Manager	Transactional Business Intelligence Receivables
Accounts Receivable Specialist	Transactional Business Intelligence Receivables
Asset Accountant	Transactional Business Intelligence Fixed Assets
Asset Accounting Manager	Transactional Business Intelligence Fixed Assets
Budget Manager	Transactional Business Intelligence Budgetary Control
Cash Manager	Transactional Business Intelligence Cash Management
Expense Manager	Transactional Business Intelligence Expenses
Financial Analyst	Transactional Business Intelligence Financials
General Accountant	Transactional Business Intelligence General Ledger
General Accounting Manager	Transactional Business Intelligence General Ledger
Intercompany Accountant	Transactional Business Intelligence Intercompany Accounting

Financials Job Role	Business Intelligence Catalog Folders
Tax Accountant	Transactional Business Intelligence Transaction Tax
Tax Administrator	Transactional Business Intelligence Transaction Tax
Tax Manager	Transactional Business Intelligence Transaction Tax
Tax Specialist	Transactional Business Intelligence Transaction Tax

Business Intelligence Reports

Analyses are secured based on the folders in which they're stored. If you haven't secured Business Intelligence reports using the report privileges, then they're secured at the folder level by default. You can set permissions against folders and reports for Application Roles, or Users.

You can set permissions to:

- Read, Execute, Write, or Delete
- Change Permissions
- Set Ownership
- Run Publisher Report
- Schedule Publisher Report
- View Publisher Output

How Reporting Data Is Secured

The data that's returned in Oracle Transactional Business Intelligence reports is secured in a similar way to the data that's returned in application pages.

Data access is granted by roles that are linked to security profiles. This topic describes the part played by Transaction Analysis Duty Roles in securing access to data in Transactional Business Intelligence reports. It also describes how to enable this access in custom job roles.

Transaction Analysis Duty Roles

Each of the Transaction Analysis Duty roles providing access to subject areas and Business Intelligence Catalog folders is granted one or more data security policies. These policies enable access to the data.

Custom Job Roles

If you create a custom job role with access to Transactional Business Intelligence reports, then you must give the role the correct duty roles. Your custom role must have both the **OBI** and **Financials** versions of the Transaction Analysis Duty roles. These duty roles ensure that your custom job role has the function and data security for running the reports.

For example, if your role must access the Fixed Asset Transaction Analysis subject areas, then it must inherit the duty roles described in the following table:

Duty Role	Version
Fixed Asset Transaction Analysis Duty	**OBI**
Fixed Asset Transaction Analysis	**Financials**

The Fixed Asset Transaction Analysis Duty role is granted relevant data security policies and inherits Business Intelligence Consumer Role.

Business Intelligence Roles

Oracle Business Intelligence roles apply to both Oracle Business Intelligence Publisher and Oracle Fusion Transactional Business Intelligence.

They grant access to Business Intelligence functionality, such as the ability to run or author reports. These roles are in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and Financials data. This topic describes the Business Intelligence roles.

This table lists the Business Intelligence roles.

Business Intelligence Role	Description
Business Intelligence Consumer Role	Allows reporting from Business Intelligence Applications, Business Intelligence Publisher, Real Time Decisions, Enterprise Performance Management and Business Intelligence Office. This role allow you to run reports from the web catalog but it will not allow a report to be authored from a subject area.
Business Intelligence Authoring	Allows authoring within Business Intelligence Applications, Business Intelligence Publisher, Real Time Decisions, Enterprise Performance Management and Business Intelligence Office.
Business Intelligence Applications Analysis	Performs Business Intelligence Applications Analysis generic duty.
Fixed Asset Business Intelligence Management	Manages access to Fixed Assets OBIA Dashboard.
Business Intelligence Applications Administrator	Provides access to the BI Applications Configuration Manager and to the BI Data Warehouse Administration Console.

Delivered Roles for Financials Subject Areas

Access to subject areas in the Oracle Business Intelligence Catalog is secured by OTBI Transactional Analysis Duty roles.

The following table lists subject areas and the corresponding job role and OTBI Transactional Analysis duty role that are required for creating user-defined reports using the subject areas. The OTBI Transactional Analysis duty role is inherited by the job role. Use this table to verify that your users have the job roles necessary to create reports using subject areas.

Note: The Business Intelligence Consumer role allows users to view reports, but not create new ones. All self-service reporting duties inherit this Business Intelligence Consumer role. All other job roles inherit the Business Intelligence Author role, enabling users with those job roles to create new reports. The following table lists subject areas for Financials and the default security roles needed for each one.

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Budgetary Control - Transactions Real Time	Budget Manager	Budgetary Control Self Service Reporting Duty	Budgetary Control Analysis Duty
• Cash Management - Bank Statement Balances Real Time • Cash Management - Bank Statement Line Charges Real Time • Cash Management - Bank Statements Real Time • Cash Management - External Cash Transactions Real Time	Cash Manager	Cash Management Self Service Reporting Duty	• Cash Management Transaction Analysis Duty
• Expenses - Employee Expense Overview Real Time • Expenses - Expense Transactions Real Time	Expense Manager	Expense Self Service Reporting Duty	• Expenses Summary Transaction Analysis Duty • Expense Transactions Transaction Analysis Duty
• Financials Common Module - Intercompany Transactions Real Time	• Intercompany Accountant • General Accountant	General Ledger Self Service Reporting Duty	Inter Company Transaction Analysis Duty
• Fixed Assets - Asset Assignments Real Time • Fixed Assets - Asset Balances Real Time • Fixed Assets - Asset Depreciation Real Time • Fixed Assets - Asset Financial Information Real Time • Fixed Assets - Asset Retirements and Reinstatements Real Time • Fixed Assets - Asset Source Lines Real Time • Fixed Assets - Asset Transactions Real Time	Asset Accountant	Fixed Asset Self Service Reporting Duty	• Fixed Asset Transaction Analysis Duty • Fixed Asset Details Transaction Analysis Duty • Fixed Depreciation Transaction Analysis Duty • Fixed Asset Details Transaction Analysis Duty

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Fixed Assets - Asset Transfer Real Time			
• General Ledger - Balances Real Time • General Ledger - Journals Real Time • General Ledger - Period Status Real Time • General Ledger - Transactional Balances Real Time	General Accountant	General Ledger Self Service Reporting Duty	• General Ledger Transaction Analysis Duty • Payables to Ledger Reconciliation Transaction Analysis Duty • Receivables to Ledger Reconciliation Transaction Analysis Duty
• Payables Invoices - Installments Real Time • Payables Invoices - Prepayment Applications Real Time • Payables Invoices - Transactions Real Time • Payables Invoices - Trial Balance Real Time • Payables Invoices - Withholding Real Time • Payables Payments - Disbursements Real Time • Payables Payments - Payment History Real Time	• Accounts Payable Manager • Accounts Payable Specialist • General Accountant	Payables Self Service Reporting Duty	• Payables to Ledger Reconciliation Transaction Analysis Duty • Payables Invoice Transaction Analysis Duty • Payables Payment Transaction Analysis Duty
• Receivables - Adjustments Real Time • Receivables - Bills Receivable Real Time • Receivables - Credit Memo Applications Real Time • Receivables - Credit Memo Requests Real Time • Receivables - Customer Account Site Tax Profile Real Time • Receivables - Customer Real Time • Receivables - Customer Tax Profile Real Time • Receivables - Miscellaneous Receipts Real Time • Receivables - Payment Schedules Real Time	• Accounts Receivable Manager • Accounts Receivable Specialist • General Accountant	Receivables Self Service Reporting Duty	• Receivables to Ledger Reconciliation Transaction Analysis Duty • Receivables Customer Transaction Analysis Duty • Receivables Transaction Analysis Duty • Receivables Receipts Transaction Analysis Duty

Subject Areas	Job Role	Self Service Reporting Duty	OTBI Transactional Analysis Duty Role
• Receivables - Receipt Conversion Rate Adjustments Real Time • Receivables - Receipts Details Real Time • Receivables - Revenue Adjustments Real Time • Receivables - Standard Receipts Application Details Real Time • Receivables - Transactions Real Time			
• Subledger Accounting - Journals Real Time • Subledger Accounting - Payables Summary Reconciliation Real Time • Subledger Accounting - Receivables Summary Reconciliation Real Time • Subledger Accounting - Supporting References Real Time	• Cash Manager • Accounts Payable Manager • Accounts Receivable Manager • Asset Accountant	• Cash Management Self Service Reporting Duty • Fixed Asset Self Service Reporting Duty • Payables Self Service Reporting Duty • Receivables Self Service Reporting Duty	Subledger Accounting Transaction Analysis Duty

Reporting Roles and Permissions

Viewing reporting roles and permissions can help you to understand how Oracle Transactional Business Intelligence security works.

This topic explains how to view:

- The reporting roles that a job role inherits
- The permissions for sample Oracle Transactional Business Intelligence reports in the Business Intelligence Catalog

Viewing Inherited Reporting Roles on the Security Console

Sign in with the IT Security Manager job role and follow these steps:

1. Select **Navigator** > **Tools** > **Security Console**.
2. On the Security Console, search for and select a job role. For example, search for and select the Accounts Payable Manager job role.

   Depending on the enterprise setting, either a graphical or a tabular representation of the role appears. Switch to the tabular view if it doesn't appear by default.

3. Accounts Payable Manager inherits many duty roles, such as Payables Balance Analysis and Payables Invoice Processing. These roles (without the word Duty in their names) are **Financials** roles. Their role codes start with the characters **ORA_**. Find these roles in the table.
4. Notice also the many Transaction Analysis Duty roles (with the word Duty in their names) that appear at the console. For example, Accounts Payable Manager inherits the Transactional Analysis Duty. These roles are **OBI** roles. Their role codes start with the characters **FBI_**. Find these roles in the table.
5. Notice that the Payables Invoice Transaction Analysis Duty role inherits BI Consumer Role. Most of the **OBI** duty roles inherit BI Consumer Role.

Tip: You can export the role hierarchy to a spreadsheet for offline review.

Viewing Permissions in the Business Intelligence Catalog

To view these permissions, you must have a role that inherits BI Administrator Role. None of the predefined Financials job roles inherits BI Administrator Role.

1. Select **Navigator** > **Tools** > **Reports and Analytics** to open the Reports and Analytics work area.
2. In the Contents pane, click the **Browse Catalog** icon. The Business Intelligence Catalog page opens.
3. In the Folders pane, expand **Shared Folders**.

   Expand the **Financials** folder and then the **Bill Management** folder.
4. Click the **Customers Export Report** folder.

   A list of reports appears on the BI Catalog page.
5. Click **Costing Reports** > **More** > **Permissions**.

   The Permissions dialog box opens. Scroll if necessary to see the complete list of permissions, which includes the role BI Administrator Role.
6. Click the Oracle Applications tab to return to the home page.

Configure Security for Oracle Transactional Business Intelligence

Oracle Transactional Business Intelligence secures reporting objects and data through a set of delivered Transaction Analysis Duty roles.

You can't configure the Transaction Analysis Duty roles provided with Oracle Financials Cloud, or the associated security privileges. However, you can configure reporting security according to your security requirements as described in this topic.

Oracle Transactional Business Intelligence secures reporting objects and data through the following types of roles:

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.
- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports and subject areas to create and run reports and view analytics.

You can't copy or modify the Business Intelligence roles or the Transaction Analysis Duty roles provided with Oracle Financials, or the associated security privileges. In addition, any role with a role code prefix of OBIA, for example,

Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS_GENERIC_DUTY), can also not be copied. However, you can configure reporting security according to your security requirements as described in this topic.

Modifying Transaction Analysis Duty Role Assignments

To configure the subject areas that users have access to create a custom job role and provide the role with the Oracle Transactional Business Intelligence duty roles that provide the required access.

For example, you can create a role that provides access to both general ledger and fixed assets subject areas by assigning both the General Ledger Transaction Analysis Duty and the Fixed Asset Transaction Analysis Duty to the role.

Modifying Business Intelligence Role Assignments

The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle Analytics Publisher. The default Business Intelligence roles used in Oracle Financials Cloud are BI Consumer and BI Author.

The delivered Transaction Analysis Duty roles inherit the BI Consumer Role, which provides view-only access to analyses and reports. You assign the BI Author Role at the job role level, giving you flexibility in granting the BI Author privilege to only those job roles that you want to have access to create and edit analyses and reports.

All predefined Financials Cloud job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default. You can optionally create copies of the predefined job roles and add or remove the BI Author Role from the roles as required.

Business Intelligence Publisher Secured List Views

Oracle Analytics Publisher is a set of tools for creating formatted reports based on data models.

You can access Analytics Publisher from Business Intelligence Composer or the Business Intelligence Catalog by clicking NewReport . This topic describes how you can use secured list views to secure access to data in Business Intelligence reports.

Some reporting tools combine the data model, layout, and translation in one report file. With that approach, business-intelligence administrators must maintain multiple copies of the same report to support minor changes. By contrast, Analytics Publisher separates the data model, layout, and translation. Therefore, reports can be:

- Generated and consumed in many output formats, such as PDF and spreadsheet
- Scheduled for delivery to e-mail, printers, and so on
- Printed in multiple languages by adding translation files
- Scheduled for delivery to multiple recipients

Analytics Publisher Data Security and Secured List Views

When you create a Analytics Publisher data model with physical SQL, you have two options.

You can:

1. Select data directly from a database table, in which case the data you return isn't subject to data-security restrictions. Because you can create data models on unsecured data, you're recommended to minimize the number of users who can create data models.
2. Join to a secured list view in your select statements. The data returned is determined by the security profiles that are assigned to the roles of the user who's running the report.

3 Implement Oracle Financials Cloud

Overview of Implementing Financials

To start your Financials implementation, use the Setup and Maintenance work area to opt into the offerings that meet your business requirements. Refer to the Oracle Applications Cloud Using Functional Setup Manager guide to manage the opt-in and setup of your offerings.

Financials Offering

By using the Financials offering, you can configure how you manage financial flows, including assets, ledgers, cash cycle, invoices and payments, accounts receivable, collections, and the setup of subledger accounting and tax configuration.

The following table specifies the primary functional areas of this offering. For the full list of functional areas and features in this offering, use the Associated Features report that you review when you plan the implementation of your offering.

Functional Area	Description
Bill Management	Manage system options and user registrations.
Budgetary Control and Encumbrance Accounting	Manage control budgets and encumbrance accounting, along with data access for users. Public sector customers typically use this functional area.
Cash Management and Banking	Manage banks, bank branches, and bank accounts. Additionally, define reconciliation matching rules, bank statement transaction creation rules, parse rules, transaction codes, and transaction type mapping. Furthermore, configure your cash positioning and cash forecasting options.
Collections	Manage aging methods and collectors, as well as collections preferences, scoring data points, and strategy tasks.
Customer Billing	Manage Receivables transactions and customer billing: AutoInvoice, payment terms, transaction types, transaction sources, memo lines, balance forward billing, and recurring billing.
Customer Payments	Manage Receivables customer payments and receipts: receipt classes and methods, AutoCash rules, Application rules, AutoMatch, Lockbox.
Expenses	Manage expense report templates, approval rules, and conversion rates and policies. If applicable, opt into using corporate cards for expenses, processing of expense receipt imaging, or integration with travel.
Financial Reporting Center	Manage the financial tools to report and analyze accounting data: Financial Reporting Center, Smart View, Financial Reporting Studio, and Workspace.

Functional Area	Description
Fixed Assets	Manage asset locations, calendars, books and categories, along with depreciation methods.
General Ledger	Manage ledgers, accounting configurations, journal sources and categories, and other related accounting setup. If applicable, opt into configuring journal approval email notifications.
Intercompany	Manage Intercompany transaction processing within Financials, intercompany balancing and reconciliation.
Joint Venture Management	Manage the distribution of joint venture revenue and costs among joint venture partners while preserving essential data for tracking and auditing.
Payables	Manage supplier invoice and payment options, payment terms, distribution sets, invoice tolerances, and procurement agents.
Payments	Manage payment systems, payment methods, formats, and payment process profiles. If applicable, opt into deriving a bank account number from IBAN.
Receivables	Manage the required setups to enable Receivables for transactions and receipts: Receivables system options; Receivables activities; AutoAccounting rules; remit-to addresses; and statement cycles.
Revenue Management	Manage system options for revenue management, selling price profiles, hierarchies, resources, and Trading Community source systems.
Revenue Recognition	Manage revenue recognition for Receivables: revenue policies and revenue contingencies.
Suppliers	Configure options for suppliers and supplier data.
Transaction Tax	Manage tax configuration, including tax regimes, taxes, and tax rates.
U.S. Federal Financials	Manage the financial management system options specifically defined for U.S. Federal agencies. **Note:** Enable U.S. Federal Financials only if you are a U.S. federal agency. When you enable U.S. Federal Financials, you incorporate processes, data elements, reporting, and accounting methods specific to federal agencies.

Related Topics

- Plan Your Implementation

Overview of the Financials Configuration for Rapid Implementation

Simplify your setup and focus only on the critical steps by using the Define Financials Configuration for Rapid Implementation task list.

The rapid implementation task list includes tasks that are:

- Critical for initial setup
- Required by most users

To create an implementation project that includes the Define Financials Configuration for Rapid Implementation task list, use the Manage Implementation Projects page in the Setup and Maintenance work area. The application implementation manager can edit the task list and assign and track each task.

Note: You can change the standard setup configuration in the rapid implementation task list. Simply add the standard Financials offering task lists and tasks to your rapid implementation project to update your setup.

Task Lists

The Define Financials Configuration for Rapid Implementation task list include the following task lists for specific functional areas within your Oracle Financials Cloud implementation:

Task List	Description
Define Common Financials Configuration for Rapid Implementation	Common configuration for Oracle Financials Cloud rapid implementation, which includes enterprise structures and banks setup.
Define Transaction Taxes for Rapid Implementation	Tax setup to address local and international tax requirements.
Define Financials Security Configuration for Rapid Implementation	User and data roles setup for Oracle Financials Cloud rapid implementation.
Define Ledger Configuration for Rapid Implementation	General Ledger rapid implementation that includes general ledger and intercompany.
Define Financial Reporting Center Configuration for Rapid Implementation	Financial Reporting Center rapid implementation that includes setup for financial reporting and integration with planning and financial management applications.
Define Invoicing and Payments Configuration for Rapid Implementation	Invoicing and payments configuration for Payables rapid implementation.
Define Expenses Configuration for Rapid Implementation	Corporate expense policies and rules, expense types, and expense report approval rules for Expenses rapid implementation.

Task List	Description
Define Fixed Assets Configuration for Rapid Implementation	Configuration for Assets rapid implementation.
Define Receivables Configuration for Rapid Implementation	Configuration for Receivables rapid implementation.

Note: Remember to perform the Open First Period task since it's required and a part of the Define Financials Configuration for Rapid Implementation task list.

Configuring Rapid Implementation Tasks Lists

Depending on the applications you're implementing, you can simplify your task lists even more. For example, if you're only implementing Receivables, you can remove the following task lists from your implementation project:

- Define Invoicing and Payments Configuration for Rapid Implementation
- Define Expenses Configuration for Rapid Implementation
- Define Fixed Assets Configuration for Rapid Implementation

Related Topics

- Example of an Oracle Financials Cloud Rapid Implementation Project

Example of an Oracle Financials Cloud Rapid Implementation Project

This example shows how to create an implementation project for the Oracle Financials rapid implementation task list.

Here are the key decisions for this example:

Decision to Consider	In This Example
What applications are included in this implementation?	You're implementing: • General Ledger • Financial Reporting Center • Payables • Receivables • Expenses • Assets

Decision to Consider	In This Example
	• Cash Management • Tax
Are the setup requirements unique to this organization?	No
Can the rapid implementation task lists and tasks be used for this implementation?	Yes

Create the Implementation Project

1. Click **Navigator** > **Setup and Maintenance**.
2. On the Setup page, open the panel tab and click **Manage Implementation Projects**.
3. On the Implementation Projects page, click the **Create** icon in the Search Results table.
4. On the Create Implementation Project: Enter Basic Information page, enter **Implementation Project-FIN_Rapid_Implementation** in the **Name** field.
5. Click in the **Description** field to automatically update the name in the description.
6. Click the **Save and Open Project** button.
7. On the Implementation Project: Implementation Project-FIN_Rapid_Implementation page, click **Add** in the Task Lists and Tasks table.
8. On the **Select and Add: Task Lists and Task** dialog box, select **Task list** in the **Search** field.
9. Enter **%Rapid Implementation%** in the **Name** field. Use wildcard characters if you don't know the exact name of the task list or task.
10. Click **Search**.
11. Select the Define Financials Configuration for Rapid Implementation row.
12. Click **Done**.
13. On the Implementation Project: Implementation Project-FIN_Rapid_Implementation page, expand the task list to see the task lists and tasks for your implementation project.
14. Click **Done**.

Common Financials Configuration

Overview of Geographies

Setting up your geography structure and master geographies correctly in the Trading Community Model is critical to the proper use and management of Oracle Enterprise Resource Planning (ERP) Cloud applications.

The geography structure and master geography data is shared across multiple product families and applications. Address validation ensures complete and valid master address data across all location entities across product applications. In addition, complete and valid master data is critical for accurate transaction tax calculation.

You can either define your geography structure and corresponding master geographies manually or import these geography entities. You can use the:

1. Manage Geographies page

2. Import Management process

For more information about managing your geographies, see the Geographies section in the Define Enterprise Structures chapter in the Oracle ERP Cloud Implementing Common Features for Financials and Project Management guide on Oracle Help Center (https://docs.oracle.com).

Manage Geographies

Use the Manage Geographies page to manually define your geography structure, hierarchy, mapping, and validation. Manually define your geographies when you have a simple geography requirement with a limited number of geographies within an individual country.

Import Management

Use the Import Management process to read the data included in your XML or text file and import the data into the application.

To access Import Management functionality, go to **Navigator** > **Tools** > **Import Management**.

For more information, see the Import Your Geography Data topic.

Related Topics

- How do I manage Geography Structures, Hierarchies, and Validation?

Implement Enterprise Structures

The Define Common Financials Configuration for Rapid Implementation task list provides a framework for developing and managing your chart of accounts, ledgers, legal entities, and business units to meet your accounting and reporting requirements.

Setting Up Enterprise Structures

The tasks in this list relate to the setup of enterprise structures. These tasks are the basic setup steps. They may be interspersed with other tasks that aren't required to implement Oracle Financials Cloud. In the Setup and Maintenance work area, create an implementation project that includes the Define Financials Configuration for Rapid Implementation task list. That task list includes the Define Common Financials Configuration for Rapid Implementation task list. Each task is performed by the Application Implementation Consultant.

> **Note:** These tasks are also included in the Define Enterprise Structures Configuration for Rapid Implementation task list, which you can add to your implementation project in the Setup and Maintenance work area.

All documentation references are from the Oracle Financials Cloud Implementing Enterprise Structures and General Ledger guide.

1. Manage geographies.
    - Perform the task **Manage Geographies** to enable the list of values for address fields in user interfaces.
    - See: Geographies chapter: Define Geographies: Overview

2. Create chart of accounts, ledger, legal entities, and business units in a spreadsheet.
    - Perform the task **Create Chart of Accounts**, **Ledger**, **Legal Entities**, **and Business Units in Spreadsheet** to create a spreadsheet for entering the primary ledger and all accompanying enterprise structures. Spreadsheet entry includes the chart of accounts with segment values and account hierarchies, associated business units, and associated legal entities. In addition, the spreadsheet includes the rules for generating sequential identifiers for transactions recorded in the application and certain setup objects along with their accounting specifications for various modules of Oracle Financials Cloud.
    - See: Financial Structures chapter
        - Enterprise Structures Rapid Implementation: Overview
        - Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheets: Explained
        - Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheets: How They're Processed
3. Upload the chart of accounts.
    - Perform the task **Upload Chart of Accounts** to load the chart of accounts structure, including segments and value sets, from the spreadsheet.
    - See: Financial Structures chapter: Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheets: How They're Processed
4. Upload the ledger, legal entities, and business units.
    - Perform the task **Upload Ledger**, **Legal Entities**, **and Business Units** to load key enterprise structures, including the ledger, legal entities, and business units that are dependent on the chart of accounts.
    - See: Financial Structures chapter: Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheets: How They're Processed.
5. Create cross-validation rules.
    - Perform the task **Create Cross Validation Rules in Spreadsheet** for the chart of accounts to determine the account combinations that users can create dynamically as they enter transactions or journal entries.
    - See: Financial Structures chapter
        - Cross-Validation Rules in General Ledger: Overview
        - Cross-Validation Rules: Explained
        - Cross-Validation Rules: Points to Consider
        - Cross-Validation Rules Spreadsheet: Explained
        - Creating Cross-Validation Rules in a Spreadsheet: Worked Example

After performing the enterprise structures tasks, run the Enterprise Structures Setup Report and diagnostic tests for the enterprise structures setup data.

- See: Enterprise Structures Introduction chapter
    - Enterprise Structures Setup Report: Explained
    - Running Diagnostic Tests for Enterprise Structures Setup Data: Explained

How You Implement Cash Management

The Oracle Fusion Cash Management product provides a framework for developing and managing your banks, bank branches, and bank accounts.

Setting Up Cash Management

The tasks in this list relate to the setup and uploading of banks, bank branches, and bank accounts. These are the basic tasks that appear in the Setup and Maintenance work area.

For setting up cash management, each task is performed by the Application Implementation Consultant. All documentation references are from the Oracle Financials Cloud Implementing Payables Invoice to Pay guide, Cash Management and Banking Configuration chapter.

1. Create banks, branches, and accounts in a spreadsheet.
    - Perform the task **Create Banks, Branches, and Accounts in Spreadsheet** to create your bank, branch, and account information.
2. Upload banks, branches, and accounts.
    - Perform the task **Upload Banks, Branches, and Accounts** to import your bank, branch, and account information into Cash Management.
    - See:
        - Cash Management Rapid Implementation: Overview

Related Topics

Implement Tax

Oracle Fusion Tax provides a single-point solution for managing your transaction and withholding tax requirements.

Oracle Fusion Tax:

- Uniformly delivers tax services to all core Oracle Fusion application business flows through one application interface.
- Provides features for uploading third-party tax partner content.
- Is configurable and scalable for adding and maintaining country-specific tax content.

Setting Up Oracle Fusion Tax

The Define Taxes for Rapid Implementation task list provides the required and most frequently used setup tasks for implementation scenarios. Using spreadsheets, you can upload your tax setups to create tax regimes, taxes, tax rates, and tax rules.

You can use the standard Define Tax Configuration task list for:

- The ongoing maintenance of your tax setup.

- Limited tax configurations that can't be set up or updated using the rapid implementation approach.

To set up Oracle Fusion Tax, the Application Implementation Consultant or Tax Manager must perform the following tasks:

1. Manage tax regimes.
    - Perform the **Manage Tax Regimes** task to create and maintain tax regimes for the taxes in each country and geographic region where a separate tax or collection of taxes apply.

      You can use the Tax Configuration Workbook to upload all common tax regime setups as well as your organization specific setups, such as tax regime subscriptions.

      You can also use the individual Tax Regimes and Tax Regime Subscriptions spreadsheets to exclusively create tax regimes and tax regime subscriptions.
    - See the following topics::
        - Tax Configuration Workbook: Explained
        - Creating Tax Setup Using the Tax Configuration Workbook: Worked Example
        - Creating Tax Setup Using Tax Partner Content in the Tax Configuration Workbook: Worked Example
        - Tax Implementation Workbook: Explained
        - Creating Tax Setup Using the Tax Implementation Workbook: Worked Example
        - Creating a Tax Regime Using the Manage Tax Regimes Spreadsheet: Worked Example
2. Run the jurisdiction and rates upload program.
    - For SaaS (Oracle Cloud) implementations, run the Import Tax Configuration Content job.
    - Refer to the Tax Configuration Content Upload Program: How It Is Processed topic.
3. Manage taxes.
    - Perform the **Manage Taxes** task to create and maintain details for the taxes of tax regimes.

      You can use the Tax Configuration Workbook to upload all common tax setups.

      You can also use the individual Taxes spreadsheet to create taxes for a tax regime or a collection of tax regimes. Additionally, you can use the individual Tax Accounts spreadsheet to create tax account assignments.
    - See the following topics:
        - Tax Configuration Workbook: Explained
        - Creating Tax Setup Using the Tax Configuration Workbook: Worked Example
        - Creating Tax Setup Using Tax Partner Content in the Tax Configuration Workbook: Worked Example
        - Creating Tax Setup Using the Tax Implementation Workbook: Worked Example
4. Manage tax rates and tax recovery rates.
    - Perform the **Manage Tax Rates and Tax Recovery Rates** task to create and maintain details for tax rates and tax recovery rates.

      You can use the Tax Configuration Workbook to upload all common tax rate and tax recovery rate setups.

      You can also use the individual Tax Rates, Tax Rate Accounts, Tax Recovery Rates, and Tax Recovery Rate Accounts spreadsheets to create:
        - Tax statuses

        - Tax jurisdictions
        - Tax rates
        - Tax recovery rates
        - Tax accounts
    - See the following topics:
        - Tax Configuration Workbook: Explained
        - Creating Tax Setup Using the Tax Configuration Workbook: Worked Example
        - Creating Tax Setup Using Tax Partner Content in the Tax Configuration Workbook: Worked Example
5. Manage tax rules.
    - Perform the **Manage Tax Rules** task to create and maintain tax rules that define the conditions under which the exceptions to the default taxability apply.

      You can use the Tax Implementation Workbook to upload organization-specific tax rule setups.

      You can also use the individual Tax Rules spreadsheet to create tax rules details.
    - See the following topics:
        - Tax Implementation Workbook: Explained
        - Creating Tax Setup Using the Tax Implementation Workbook: Worked Example
6. Manage tax registrations.
    - Perform the **Manage Tax Registrations** task to create and maintain tax registration information related to a party's transaction tax obligation with a tax authority for a tax jurisdiction where it conducts business.

      You can use the Tax Implementation Workbook to upload your organization-specific tax registrations.
    - Refer to the Tax Registrations: Explained topic.
7. Manage tax exemptions.
    - Perform the **Manage Tax Exemptions** task to create and maintain tax exemptions to reduce or increase the tax rate applied to a transaction.
    - Refer to the Tax Exemptions: Explained topic.
8. Manage simulator transactions.
    - Perform the **Manage Simulator Transactions** task to verify tax configuration for taxes that are enabled for simulation or for both simulation and transactions by processing real-time transactions without affecting active data.
    - Refer to the Tax Simulator: Explained topic.

Related Topics

- Implementing Tax

Implement U.S. Federal Financials

Get started with Oracle U.S. Federal Financials to enable your agency to meet Federal financial management system requirements. To complete setting up U.S. Federal Financials, you must complete the core setup steps along with the necessary prerequisite setups for the integrated applications.

Setting Up U.S. Federal Financials

The tasks in this list include the setup steps for U.S. Federal Financials. These tasks are performed by the Financial Applications Administrator.

1. Prerequisites
    - Manage users
        - Perform the task **Manage Users** to create users and assign access privileges.
    - Manage chart of accounts structures
        - Perform the task **Manage Chart of Accounts Structures** to define accounting flexfields and Federal-specific segment labels.
    - Manage invoice options
        - Perform the task **Manage Invoice Options** to control how invoices are processed for your business unit.
    - Manage accounting calendars
        - Perform the task **Manage Accounting Calendars** to create Federal-specific accounting calendar
2. Core Federal Financials Setup
    - Manage federal options
        - Perform the task **Manage Federal Options** to define the business unit attributes for each business unit of your agency.
    - Manage federal account symbols
        - Perform the task **Manage Federal Account Symbols** to define Federal account symbols for your agency.
    - Manage agency location codes
        - Perform the task **Manage Agency Location Codes** to define Treasury-assigned codes that identify the accounting and reporting offices of your agency.
    - Manage treasury account symbols
        - Perform the task **Manage Treasury Account Symbols** to define identification codes for individual appropriations, receipts, and other fund accounts of your agency.
    - Manage fund attributes
        - Perform the task **Manage Fund Attributes** to define fund attributes used by your Federal agency for Treasury reporting and legal compliance.

3. Subledger Accounting Setup
    - Define expense accrual distributions
        - Perform the task **Manage Mapping Sets** for Procurement offering to define the expense accrual distributions for the Purchasing accounts for your agency.
    - Define General Ledger accounts
        - Perform the task **Manage Mapping Sets** for Accounting Hub offering to define the General Ledger accounts used by Subledger Accounting for your agency.
4. Prompt Payment Setup
    - Define transaction calendar
        - Perform the task **Manage Transaction Calendars** to define a transaction calendar for Prompt Payment processes.
    - Define lookups
        - Perform the task **Manage General Ledger Lookup Values** to define lookup codes for Prompt Payment processes.
    - Define current value of funds rate
        - Perform the task **Manage Interest Rates** to define the rate of interest applicable on your overdue invoices.
    - Define payment terms
        - Perform the task **Manage Payment Terms** to define invoice payment terms that comply with the Prompt Payment Act.
5. Payment Processing Setup
    - Define pay group lookups
        - Perform the task **Manage Payables Lookups** to define a pay group that maps to the payment format of a payment type.
    - Define payment type mappings
        - Perform the task **Manage Payment Type Mapping** to map a payment type to a pay group.
    - Define internal bank branches
        - Perform the task **Manage Bank Branches** to define the bank branches for internal bank accounts.
    - Define internal bank accounts
        - Perform the task **Manage Bank Accounts** to define bank accounts that recognize the Secure Payment System or Payment Automation Manager format.
    - Define payment process request templates
        - Perform the task **Manage Payment Process Request Templates** to define the payment process request templates.

Related Topics

Ledger Configuration

Implement General Ledger

The Define Ledger Configuration for Rapid Implementation and Define Financial Reporting Center Configuration for Rapid Implementation task lists provide a framework for developing and managing general ledger features including ledger sets, journal approval rules, and the Financial Reporting Center.

Setting Up General Ledger

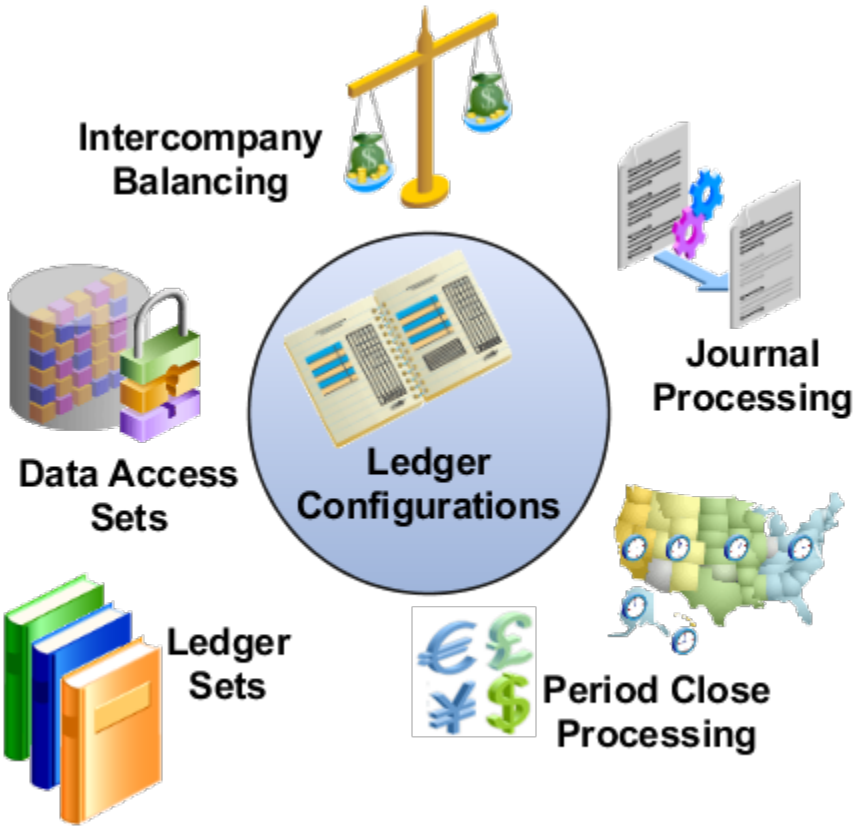
The tasks in the following list relate to the setup of General Ledger. These tasks are the basic setup steps. They may be interspersed with other tasks that aren't required to implement Oracle Financials Cloud. In the Setup and Maintenance work area, create an implementation project that includes the Define Financials Configuration for Rapid Implementation task list. That task list includes both the Define Ledger Configuration for Rapid Implementation and Define Financial Reporting Center Configuration for Rapid Implementation task lists.

For setting up general ledger, each task is performed by the Application Implementation Consultant.

Define Ledger Configuration for Rapid Implementation

All documentation references are from the Oracle Financials Cloud Implementing Enterprise Structures and General Ledger guide, unless otherwise noted.

This image shows the general categories of ledger configuration: intercompany balancing, journal processing, period close processing, ledger sets, data access sets, and intercompany balancing.



1. Manage ledger sets.
    - Perform the task **Manage Ledger Sets** to create, review, and update collections of ledgers intended for batch processing or financial reports.
    - See: Ledgers chapter
        - Ledgers and Subledgers
        - Primary Ledgers, Secondary Ledgers, and Reporting Currencies
        - Ledgers, Legal Entities, Balancing Segments, and Business Units
2. Manage data access sets.
    - Perform the task **Manage Data Access Sets** to create, review, and update collections of ledgers intended for data security.
    - See: Financial Structures chapter
        - Overview of General Ledger Security
        - Overview of Data Access Set Security
        - Examples of Data Access Set Security

3. Create segment value security rules.
    - Go to the Manage Chart of Accounts Configurations page to define segment value security for chart of accounts value sets.
    - See: Financial Structures chapter
        - Overview of General Ledger Security
        - Overview of Segment Value Security
        - Enforcement of Segment Value Security by Business Function
4. Manage intercompany balancing rules.
    - Perform the task **Manage Intercompany Balancing Rules** to define rules to assign intercompany receivables and intercompany payables accounts for transactions unbalanced by legal entity or management entity.
    - See: Intercompany Setup chapter
        - Intercompany Balancing Rules
        - Intercompany System Options
        - Example of Intercompany Organization Configuration
        - Customer and Supplier Assignment
5. Manage journal approval rules.
    - Perform the task **Manage Journal Approval Rules** to review and update rules to route journal entries through an approval process.
    - See: General Ledger Options chapter
        - Considerations for Defining Journal Approving Rules
        - Create Journal Approval Rules
6. Manage settings for automatic journal posting.
    - Perform the task **Manage AutoPost Criteria Sets** to define, review and update settings for automatic journal posting.
    - See: General Ledger Options chapter
        - Create an AutoPost Criteria Set
        - Examples of Manually Running the AutoPost Process
7. Manage settings for automatic journal reversal.
    - Perform the task **Manage Journal Reversal Criteria Sets** to define, review, and update settings for automatic journal reversal.
    - See: General Ledger Options chapter, Journal Reversals
8. Manage accounting and reporting sequences.
    - Perform the task **Manage Accounting and Reporting Sequences** to define, review, and update sequencing definitions for journal posting and period close.
    - See: General Ledger Options chapter
        - Overview of Accounting and Reporting Sequences
        - How to Define Journal Sequences Manually: Explained
        - What happens when I enable sequencing in the rapid implementation spreadsheet?

9. Manage allocations and periodic entries.
    - Perform the task **Manage Allocations and Periodic Entries** to create, review, and update allocation and periodic definitions and journal entries. Generate journal entries from the allocation and periodic definitions.
    - See: Allocations and Periodic Entries chapter
        - Overview of Allocations and Periodic Entries
        - Overview of Calculation Manager
        - Overview of Oracle Essbase Balances Cubes
        - Create an Allocation Rule and Generate Allocations
        - Overview of Recurring Journals
10. Manage revaluation definitions.
    - Perform the task **Manage Revaluations** to review and update existing calculations of unrealized gains and losses on foreign currency transactions, and to define new calculations.
    - See: Period Close chapter
        - Revaluation Process
        - Overview of Revaluation Unrealized Gains or Losses
        - How Income Statement Accounts Are Revalued
        - Overview of Revaluation Tracking By Multiple Segments
11. Manage historical rates.
    - Perform the task **Manage Historical Rates** to review and update existing currency historical conversion information, and to create conversion information.
    - See: Financial Structures chapter
        - Enter Daily Rates Using the Daily Rates Spreadsheet
        - Update Currency Rates
12. Open the first period.
    - Perform the task **Open First Period** to open the first accounting period so you can begin recording transactions.
    - See: Ledgers chapter: Overview of Opening First Period
    - See: Period Close chapter: Overview of Close Monitor

Define Financial Reporting Center Configuration for Rapid Implementation

All documentation references are from the Oracle Financials Cloud Implementing Enterprise Structures and General Ledger guide, Financial Reporting chapter, unless otherwise noted.

1. Define Financial Reporting Center configuration:
    - Perform the tasks in the Define Financial Reporting Center Configuration task list to define and manage technical configuration options for the Financial Reporting Center.
    - See:
        - Overview of Financial Reporting Center
        - Set Up Financial Reporting Center and Smart View

2. Define Essbase database connections.
    - Perform the task **Define Essbase Database Connections in Workspace** to define database connections to connect to Essbase in Workspace.
    - See: Set Up Financial Reporting Center and Smart View
3. Configure the Smart View client.
    - Perform the task **Configure Smart View Client for Users** to install the Smart View client on users' computers to perform balance inquiry.
    - See: Set Up Financial Reporting Center and Smart view
4. Create financial statements.
    - Perform the task **Create Financial Statements** to create, review, and update report definitions for management and statutory financial statements.
    - See: Create a Financial Report
5. Define budget scenarios.
    - Perform the task **Define Budget Scenarios** to define scenarios to track budgets for different periods or forecasts.
    - See: Budgets chapter
        - Overview of Budget Uploads
        - How General Ledger Budget Balance Import Data Is Processed
        - Import Budget Data from a Flat File
        - Import Budget Data from a Spreadsheet

Related Topics

Intercompany Balancing Rules

You use Intercompany balancing rules to generate the accounts required to balance journals that are out of balance by legal entity or primary balancing segment values.

Specify the intercompany receivables and intercompany payables accounts that you want to use as the template for building the intercompany receivables and intercompany payables accounts. The intercompany balancing feature then uses these rules to generate the accounts of the balancing lines it creates.

Journals lines are first summarized by the legal entity and are balanced by the legal entity. Since a legal entity can have many primary balancing segment values, it's possible that a journal could have multiple lines for a legal entity with different primary balancing segment values. In that case, when intercompany balancing is done, the lowest primary balancing segment value within each legal entity in the journal is used. After this, balancing occurs across balancing segment values within each legal entity.

These same rules are also used to generate the intercompany receivables account and intercompany payables account of transactions entered in the Intercompany module.

The intercompany balancing rules are also used to generate the intercompany receivables account for the provider side of an intercompany transaction. And balancing rules are also used to generate the intercompany payables account for the receiver side of an intercompany transaction.

CAUTION: After you create an Intercompany balancing rule, you can't modify them. But you can end date an existing rule and create a new rule.

Defining Intercompany Balancing Rules

You can define intercompany balancing rules at these levels:

1. Primary balancing segment
2. Legal entity
3. Ledger
4. Chart of accounts

The rules are evaluated in the order shown. For example, you can define a Primary Balancing Segment rule and a Legal Entity level rule. If both rules can be used to balance a particular journal, the Primary Balancing Segment rule is used, as it has a higher precedence.

You have flexibility in defining your intercompany balancing rules. You can have a simple setup in which you define one rule for your chart of accounts. This rule is used for all intercompany balancing for all ledgers that use this chart of accounts. Alternatively, you can have a more granular set of rules. For example, define a different rule for each legal entity and one chart of accounts rule to cover any gaps. You can gain even more granularity by defining rules for specific journal and category combinations or intercompany transaction types.

Using Chart of Accounts Rules for Intercompany

Use chart of accounts rules for intercompany balancing. You have flexibility in defining your intercompany balancing rules with the setup of a single chart of accounts rule to use for all ledgers that use this chart of accounts. When you create a chart of accounts rule, you specify the chart of accounts, intercompany receivables, and intercompany payables accounts you want to use, as well as the source and category. It is recommended that the intercompany receivables account be an asset type account, and the intercompany payables account be a liability type account.

You can define rules that are applied to a specific source and category, such as Payables and Invoices. Or a specific intercompany transaction type, such as Intercompany Sales. Alternatively, you can choose to create rules for all sources and categories by selecting the source of **Other** and the category of **Other**.

Intercompany Balancing then evaluates the journal source and journal category combination in determining which rule to use for balancing. This is the order of precedence.

- Specific journal source and journal category
- Specific journal source and journal category of Other
- Journal source of Other and specific journal category
- Journal source of Other and journal category of Other

Additional Intercompany Balancing and Clearing Company Options

Additional Intercompany Balancing and Clearing options are used to balance the second balancing segment or the third balancing segment or both, when a transaction is unbalanced by one of these segments but is already balanced by the primary balancing segment. This option is defined for a ledger but you can create rules for various Source and Category combinations.

Additional Intercompany Balancing and Clearing options include these settings:

- Intercompany Receivables and Intercompany Payables accounts: You can use as the accounts as the template to build balancing accounts for balancing segment 2 and balancing segment 3 when the journal is already balanced by primary balancing segment.
- Summarization options: You can choose to summarize lines within a legal entity before balancing lines are generated by choosing the Summary Net option. Alternatively choose the Detail options so lines aren't summarized before balancing within a legal entity. Note that summarization always applies to balancing lines generated in a cross legal entity scenario.
- Clearing company options: Oracle recommends to always set clearing company options to handle many-to-many journals. This avoids balancing failing during General Ledger Posting or Subledger Accounting Create Accounting process.

Clearing Company Options

You can choose to set clearing company options to balance a many-to-many journal. Set these options to manage your clearing company balancing.

- Clearing Company Condition: Choose when to use a clearing company.
    - Use clearing company only for intracompany journals.
    - Use clearing company for all many-to-many journals.
    - Error out if many-to-many journal. The default value for this option.
- Clearing Company Source: Choose how the clearing company value is derived for your balancing lines, from these options:
    - Default clearing balancing segment value.
    - Manually entered clearing balancing segment value. Note that if you select Manually entered clearing balancing segment value, then you must manually enter a value in the create journals screen. This option doesn't work for subledger accounting entries as they don't have a field on the user interface to enter this value.
- Clearing Company Value: If you selected Default clearing balancing segment value for Source, you must select a primary balancing segment value in this field. This value is used to balance your intracompany or many-to-many journals.

Example of Intercompany Balancing Rules

This topic provides examples of intercompany balancing rules and the intercompany balancing lines generated. These rules are used to generate the accounts needed to balance journals that are out of balance by legal entity or primary balancing segment values.

Intercompany Balancing Rules Precedence

In this example the legal Entity InFusion Textiles intercompany manufacturing activities are tracked separately from its non-manufacturing activities. To achieve this, legal entity level rules are defined specifically between the legal entity

InFusion Textiles and the two manufacturing legal entities, InFusion Products (East) and InFusion Products (West). A chart of accounts rule is created to cover all other intercompany activities.

Setup

- InFusion USA Chart of Accounts as shown in this table.

Segment Name	Company (CO)	Cost Center (CC)	Division (DIV)	Account (ACCT)	Intercompany (IC)
Segment Qualifier	Primary Balancing Segment	Second Balancing Segment	Third Balancing Segment	Account	Intercompany Segment

- Ledger, Legal Entity, Primary Balancing Segment Value Assignments as shown in this table.

Ledger	Legal Entity	Primary Balancing Segment Value
InFusion USA	InFusion Farms	3100, 3200, 3300, 3400, 3500
InFusion USA	InFusion Textiles	4000
InFusion USA	InFusion Products (East)	5000
InFusion USA	InFusion Products (West)	6000
InFusion USA		1000, 9000

- Chart of Accounts Rule as shown in this table.

Rule Number	Chart of Accounts	AR Account	AP Account	Source	Category	Transaction Type
1	InFusion USA Chart of Accounts	1000 - 000 - 0000 - 13050 - 0000	1000 - 000 - 0000 - 21050 - 0000	Other	Other	None

- Legal Entity Level Rule as shown in this table.

Rule No.	From Legal Entity	To Legal Entity	AR Account	AP Account	Source	Category	Transaction Type
2	InFusion Textiles	InFusion Products (West)	1000 - 000 - 0000 - 13020 - 0000	1000 - 000 - 0000 - 21020 - 0000	Other	Other	None
3	InFusion Textiles	InFusion Products (East)	1000 - 000 - 0000 - 13030 - 0000	1000 - 000 - 0000 - 21030 - 0000	Other	Other	None

Rule No.	From Legal Entity	To Legal Entity	AR Account	AP Account	Source	Category	Transaction Type

- Journal Balancing
  - Journal before Balancing as shown in this table.

Line	Line Type	Legal Entity	CO	CC	DIV	ACCT	IC	Debit	Credit
1	Expense	InFusion Farms	3100	100	1200	52330	0000	150	
2	Expense	InFusion Products (East)	5000	100	1200	52340	0000	200	
3	Expense	InFusion Products (West)	6000	200	1300	52345	0000	300	
4	Liability	InFusion Textiles	4000	500	1300	40118	0000		650

- Journal Balancing
  - Journal after Balancing as shown in this table.

Uses Rule	Line	Line Type	Legal Entity	CO	CC	DIV	ACCT	IC	Debit	Credit
	1	Expense	InFusion Farms	3100	100	1200	52330	0000	150	
	2	Expense	InFusion Products (East)	5000	100	1200	52340	0000	200	
	3	Expense	InFusion Products (West)	6000	200	1300	52345	0000	300	
	4	Liability	InFusion Textiles	4000	500	1300	40118	0000		650
1	5	IC AR	InFusion Textiles	4000	500	1300	13050	3100	150	

Uses Rule	Line	Line Type	Legal Entity	CO	CC	DIV	ACCT	IC	Debit	Credit
1	6	IC AP	InFusion Farms	3100	100	1200	21050	4000		150
3	7	IC AR	InFusion Textiles	4000	500	1300	13030	5000	200	
1	8	IC AP	InFusion Products(Ea	5000	100	1200	21050	4000		200
2	9	IC AR	InFusion Textiles	4000	500	1300	13020	6000	300	
1	10	IC AP	InFusion Products (West)	6000	200	1300	21050	4000		300

Related Topics

- Intercompany Balancing Rules

Invoicing and Payments Configuration

How You Implement Payables and Payments

The Invoicing and Payments Configuration for Rapid Implementation task list provides the framework for managing essential setups for Oracle Payables and Oracle Payments.

The framework includes setups for Oracle Procurement that are required for Payables. It also provides the setup steps for common options, distribution sets, and invoice tolerances for Payables, and the setup steps of disbursement system options, payment methods, and payment process profiles for Payments.

Setting Up Payables and Payments

The tasks in the following list relate to the setup of Payables and Payments.

For setting up Payables and Payments, each task is performed by the Application Implementation Consultant. References to help topics in the following tasks are from the following publications:

- Oracle Financials Cloud Implementing Payables Invoice to Pay
  - General Payables Options chapter, Manage Common Options for Payables and Procurement section
  - Payables Configuration chapter
  - Disbursements chapter
- Oracle Procurement Cloud Implementing Procurement

    - Purchasing Configuration chapter, Define Procurement Agents section

- Oracle Procurement Cloud Using Procurement
    - Supplier Profiles chapter, Create Supplier section
    - Supplier Profiles chapter, Import Suppliers section

1. Configure Procurement business function, procurement agents, and suppliers.
    - Perform the task **Configure Procurement Business Function, Procurement Agents, and Suppliers**, which includes configuring:
        - The procurement business function for the procurement business unit to specify procurement document control, document defaults, document numbering, and related settings.
        - Procurement agent access to information, such as purchasing documents and suppliers.
        - Suppliers, sites, and other supplier-related information.
    - See: Define Procurement Agents section
        - Procurement Agents
    - See: Supplier Profiles chapter
        - Oracle Supplier Model
        - Import Suppliers section
        - See: Create Supplier section
            - Supplier Sites and Supplier Site Assignments: Explained
2. Manage common options for Payables and Procurement.
    - Perform the task **Manage Common Options for Payables and Procurement** to set the controls and default values that are used by both Payables and Procurement, such as the default liability account and whether to accrue expense items at time of receipt or at period end.
    - See: Manage Common Options for Payables and Procurement section
        - Guidelines for Common Options for Payables and Procurement
        - Default Distributions
        - Considerations for Offset Segments
        - Considerations for Accruing Expense Items

    > **Note:** You can skip this step if you have used the Rapid Implementation spreadsheet for General Ledger to create the ledger, legal entities, and business units.

3. Manage distribution sets.
    - Perform the task **Manage Distribution Sets** to define a distribution set, which is a list of accounts with or without percentages. When you create an invoice that's not associated with a purchase order, you can enter the distribution set name to automatically create the invoice distributions with a predefined set of accounts. If the distribution set has percentages, the invoice line amount is automatically distributed to the accounts, otherwise you must enter the amounts manually.
    - See: Payables Configuration chapter
        - Distribution Sets
4. Manage invoice tolerances.

- Perform the task **Manage Invoice Tolerances** to define acceptable variances between invoice, purchase order, and receipt information. You can define both percentage-based and amount-based tolerances. Invoices that exceed the specified tolerances are placed on hold during the invoice validation process.
- See: Payables Configuration chapter
  - Invoice Tolerances

5. Manage disbursement system options.

> **Note:** Payments provides predefined setups for Steps 5 to 7. You don't need to modify the predefined setups unless you want to change disbursement system options, or configure different payment methods or payment process profiles.

- Perform the task **Manage Disbursement System Options** to manage payment processing options at the enterprise and business unit level.

6. Manage payment methods.

- Perform the task **Manage Payment Methods** to define or manage payment methods and to attach or update validations that are assigned to them. See:
  - Payment Methods
  - Payment Method Defaulting
  - Example of Setting Up User-Defined Validations for Payment Methods or for Payment Files

7. Manage payment process profiles.

- Perform the task **Manage Payment Process Profiles** to define or manage payment process profiles, which are entities that determine the payment processing type, grouping of installments, grouping of payments, and the definition of usage rules based on payment methods, disbursement bank accounts, business units, and currencies. See:
  - Payment Process Profiles

Related Topics

Expenses Configuration

Implement Expenses

The Define Expenses Configuration for Rapid Implementation task list provides a framework for developing and managing your system options, expense report templates, approval rules, and conversion rates and policies.

The tasks in the Define Expenses Configuration for Rapid Implementation task list enable expense entry, approval, and reimbursement processing in Expenses.

Setting Up Expenses

To set up Expenses, each task is performed by the Application Implementation Consultant. References to help topics in the following tasks are from the Oracle Financials Cloud Implementing Expenses: Expense Policies and Rules chapter.

1. Manage expenses system options.
    - Perform the task **Manage Expenses System Options** to define setup options for managing expense entry and processing for all business units.
    - Confirm that the default settings are aligned with your business practices.
2. Manage expense report templates.
    - Perform the task **Manage Expense Report Templates** to define expense types applicable to your company and group them into expense templates. Expense templates are defined by business units. The expense templates available in expense report entry is determined by the business unit of the employees.
    - Specify receipt requirements when you define expense types.
    - See:
        - Expense Templates: Points to Consider
        - Can expense types be used across expense templates?
        - Configuring Expense Policies: Points to Consider.
3. Manage expense approval rules.
    - Perform the task **Manage Expense Approval Rules** to define expense report approval rules based on your company's approval policies.
    - Modify the predefined rules as needed.
    - See:
        - Configuring Approval Rules: Explained
        - Defining Approval Rules: Explained

    Note: To enable audit of expense reports, you must define audit rules in addition to approval rules.
4. Manage conversion rates and policies.
    - Perform the task **Manage Conversion Rates and Policies** to select the conversion rate type for each business unit.
    - See: Configuring Expense Policies: Points to Consider

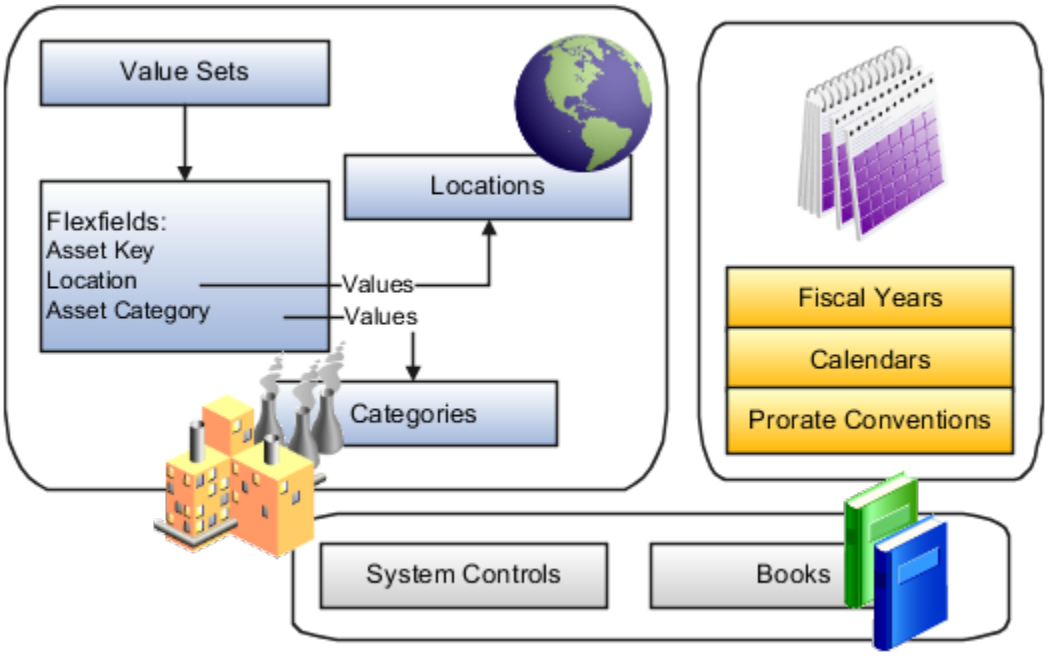
Related Topics

Fixed Assets Configuration

Implement Assets

Get started with Oracle Assets and enable your reporting and accounting capabilities using the Define Fixed Assets Configuration for Rapid Implementation task list.

This task list provides a framework to develop and manage your Assets flexfields, system controls, fiscal years, locations, calendars, prorate conventions, asset books, and asset categories.



Set Up Assets

The tasks in the following list relate to the setup of Oracle Assets. These are the basic steps for setup. These tasks appear in the setup task list in the Setup and Maintenance work area. However, in your task list the tasks may be interspersed with other tasks that you don't need to perform before you can use Oracle Fusion Cloud Financials.

For setting up Assets, each task is performed by the Application Implementation Manager.

Define Fixed Assets Configuration for Rapid Implementation

All documentation references are from the Oracle Financials Cloud Implementing Assets guide, unless otherwise noted.

1. Create Fixed Assets Configuration in Spreadsheet.
    - Perform the task **Create Fixed Assets Configuration in Spreadsheet** to define your initial Fixed Assets configuration or rapidly implement Oracle Asset categories, system controls, depreciation calendars, prorate conventions, and books.
    - See: Oracle Applications Cloud Configuring and Extending Applications guide.
2. Update Fixed Assets Configuration in Spreadsheet.
    - Perform the task **Update Fixed Assets Configuration in Spreadsheet** to update or add to your Oracle Asset categories, locations, and books.
3. Upload Fixed Assets Configuration in Spreadsheet.
    - Perform the task **Upload Fixed Assets Configuration in Spreadsheet** to load the key flexfield structure, system controls, calendar, prorate convention, asset book, location combination, and category assignment to the book created or updated in the spreadsheet.

> **Note:** For an example of using configuration packages in Oracle Assets, see *Technical Brief: Fusion Assets Configuration Package Creation (KB98505)* on My Oracle Cloud Support.

Related Topics

- System Controls
- Depreciation Methods
- How You Use Implementation Projects to Manage Setup

Receivables Configuration

Implementation Procedures for Receivables and Payments

The Receivables task list provides a framework for developing and managing your accounts receivable environment. This includes the necessary setups in Oracle Receivables and the related setups in Oracle Payments.

Define the Receivables and Payments Configuration

The tasks in the following list relate to the setup of Receivables and of Payments for Receivables. These are the basic steps for setup.

For setting up Receivables and Payments for Receivables, each task is performed by the Application Implementation Consultant. All documentation references are from these chapters in Oracle Financials Cloud Implementing Receivables Credit to Cash:

- Define Common Accounts Receivable Configuration
- Manage Receivables System Options
- Define Customer Billing Configuration
- Define Customer Payments
- Configure Payment System Connectivity
- Define Funds Capture
- Define Customer

1. Manage Receivables system options.
    - Perform the task **Manage Receivables System Options** to manage the basic settings of your Receivables environment.
    - See: Manage Receivables System Options chapter:
        - Updating System Option Records: Critical Choices
        - Using Header Level Rounding: Example
        - Tax Invoice Printing Options
        - Tuning Segments: Explained
        - Log File Message Levels: Explained
        - Transaction and Statement Delivery E-Mail Subject Line: Examples
        - Transaction and Statement Delivery Using E-Mail: How It Works
2. Manage Receivables activities.

- Perform the task **Manage Receivables Activities** to set up default accounting information for all activities in accounts receivable other than transaction processing and receipt processing.
- See: Define Common Accounts Receivable Configuration: Define Receivables Activities section:
  - Receivables Activity Types
  - GL Account Source
  - Tax Rate Code Source

3. Manage AutoAccounting rules.
   - Perform the task **Manage AutoAccounting Rules** to set up default accounting information for Receivables transaction processing.
   - See: Define Customer Billing Configuration: Define AutoAccounting section:
     - AutoAccounting Account Types and Segment Values
     - AutoAccounting Structure: Points to Consider
     - Using AutoAccounting to Derive Accounting Flexfield Segments: Example
4. Manage remit-to addresses.
   - Perform the task **Manage Remit-to Addresses** to assign remit-to addresses to Receivables transactions.
   - See: Define Customer Billing Configuration: FAQs for Remit-to Addresses section:
     - How can I use remit-to addresses?
     - How does AutoInvoice validate remit-to addresses?
     - How can I define a default remit-to address?
     - Why did the country appear?
     - Why do I verify the address?
5. Manage memo lines.
   - Perform the task **Manage Standard Memo Lines** to define memo lines for line items that aren't inventory items.
   - See: Define Customer Billing Configuration: Define Memo Lines section: Revenue Accounts and Memo Lines: Explained.
6. Manage system security options.
   - Perform the task **Manage System Security Options** to enable the credit card and bank account encryption and masking.
   - See: Define Payments Security chapter: System Security Options: Critical Choices.
7. Manage funds capture payment methods.
   - Perform the task **Manage Funds Capture Payment Methods** to define funds capture payment methods to enable customers to remit payments. Payments supports bank account transfers for automated funds capture processing.
8. Manage funds capture process profiles.
   - Perform the task **Manage Funds Capture Process Profiles** to define profiles for funds capture processing with rules for authorization and settlement handling.
   - See: Define Funds Capture chapter: Funds Capture Process Profile: Explained.

9. Manage internal payees.
    - Perform the task **Manage Internal Payees** to set up one or more business units that use a payment processor or gateway to receive funds from customers.
10. Manage payment systems.
    - Perform the task **Manage Payment Systems** to define external organizations, such as banks or payment processors, that process funds capture and disbursement transactions.
    - See: Configure Payment System Connectivity chapter:
        - Validations: Critical Choices
        - Formats: Explained
        - Transmission Protocol: Explained
        - Transmission Configuration: Explained
        - Configuring Your Communication Channel to a Payment System: Explained
        - Payment System: Explained
        - Payment System Account: Explained
        - Importing a Security Credential File: Procedures
11. Manage receipt classes and methods.
    - Perform the task **Manage Receipt Classes and Methods** to set up the steps required for receipts and to set up default accounting information for receipt processing.
    - See: Define Customer Payments: Define Receipt Classes and Methods section:
        - Remittance Methods and Clearance Methods
        - Automatic Receipt Processing: Points to Consider
        - Fund Transfer Error Handling: Explained
        - Remittance Bank Accounts: Explained
12. Manage lockbox.
    - Perform the task **Manage Lockbox** to set up a lockbox to create receipts automatically from data supplied by your remittance bank.
    - See: Define Customer Payments: Define Lockbox section:
        - Lockbox Interface Table AR_PAYMENTS_INTERFACE_ALL
        - Match Receipts By Method: Explained
13. Manage transmission formats for lockbox.
    - Perform the task **Manage Transmission Formats for Lockbox** to set up lockbox transmission formats. The transmission formats ensure that data is correctly transferred from your remittance bank.
    - See: Define Customer Payments: Define Transmission Formats for Lockbox section:
        - Validating the Lockbox File Transmission: How It Works
        - Lockbox Transmission Formats
        - Lockbox Transmission Format Record Types
        - Lockbox Transmission Format Field Types
14. Manage statement cycles.
    - Perform the task **Manage Statement Cycles** to set up statements and statement cycles that determine when to send statements to your customers.
    - See: Define Common Accounts Receivable Configuration: Define Statements section:

        - Setting Up for Statements: Procedure
        - Statement Cycles: Example

15. Create customer.

    - Perform the task **Create Customer** to create customer records for all organizations and persons with whom you do business.
    - See: Define Customer chapter: Define Customer Account section and Manage Customers section:

        - Customer Account Relationships: Explained
        - Customer Account Uses: Points to Consider
        - Customer Addresses: Points to Consider
        - Related Contact Sites: Explained
        - Customer and Party: Explained
        - Party Relationships: Explained
        - Customer Upload: How Data is Processed
        - Preparing Customer Data for Upload: Points to Consider
        - Validating Unique Values in the Customer Spreadsheet Upload: Examples
        - Customer Listing Report

16. Manage approval limits.

    - Perform the task **Manage Approval Limits** to set approval limits for each of your users for specific transactions and amount ranges per currency.
    - See: Define Common Accounts Receivable Configuration: Define Approval Limits section: Approval Limits Document Types.

Related Topics

4 Financial Reporting

Overview of Financial Reporting Configuration

Configure these financial tools to report and analyze your accounting data: Financial Reporting Center, Smart View, Financial Reporting Studio, and Workspace.

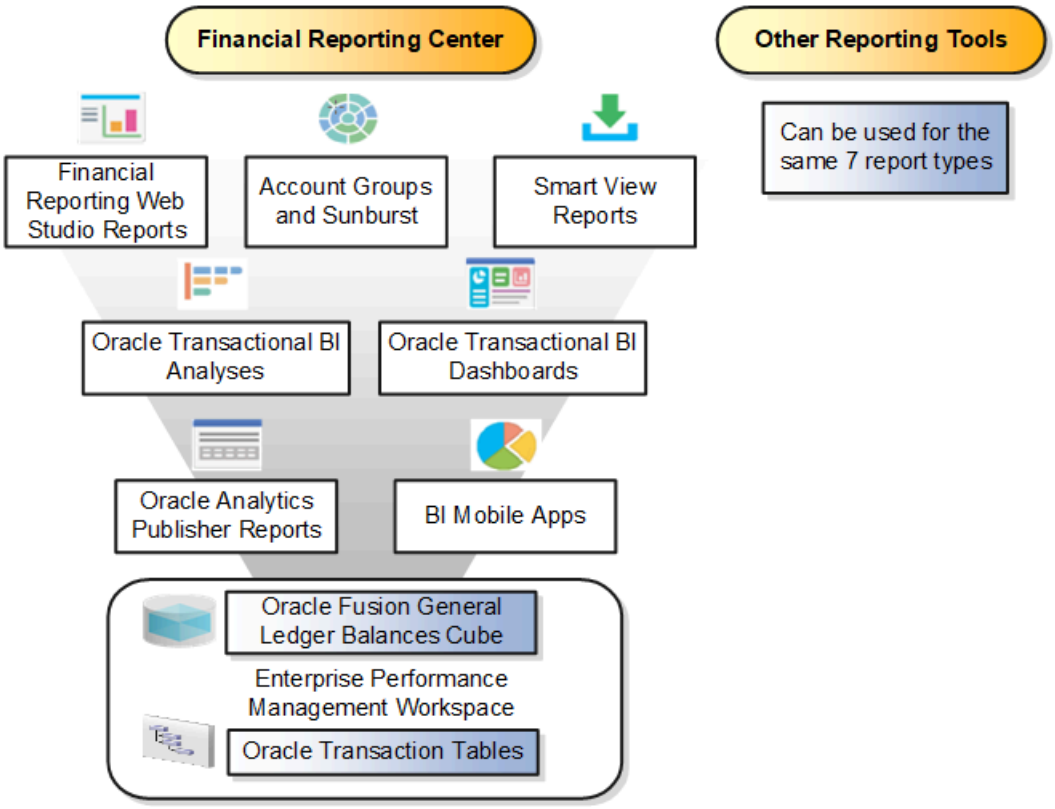
Overview of Financial Reporting Center

The Financial Reporting Center is intended to be the primary user interface for financials end users to access all seven report types.

Financial Reporting Center

The Financial Reporting Center includes these report types: Financial Reporting Web Studio Reports, Account Groups and Sunburst, Smart View Reports, Oracle Transactional Business Intelligence Analyses, Oracle Transactional Business Intelligence Dashboards, Oracle Analytics Publisher Reports, and Business Intelligence Mobile Apps. Other reporting tools are also available to run the same seven report types.

This figure illustrates the report types that are available in the Financial Reporting Center.



Reports can be accessed through various methods. However, the Financial Reporting Center provides access to every type of report, is intended to be the primary user interface for financials end users, and is tablet and smartphone friendly. In addition to accessing reports, you can add favorites, define tags, and view report details, such as type and last updated date.

Financial Reports are read from the **Shared** > **Custom** > **Financials** and **My Folders** directories. All other report types can be saved anywhere in the BI Catalog however, any user-defined content should be in the **Shared** > **Custom** folder. Subfolders can be created within the **Shared** > **Custom** folder.

Seven types of reports can be run from the Financial Reporting Center and from the other reporting tools.

- Financial Reports: These reports are built off of the Oracle Financial Reporting Web Studio using data in the Oracle General Ledger balances cube. For example, company income statements and balance sheets. These reports are mainly run by users in General Ledger.
- Account Groups and Sunburst: Account groups are used to monitor key accounts in General Ledger. When a user creates an account group, it becomes visible in the Financial Reporting Center with the Sunburst visualization tool. The Sunburst visualization tool lets you interact with your account balances across various business dimensions to view balances from different perspectives. Account groups are used only in General Ledger.
- Smart View Reports: Smart View is a multidimensional pivot analysis tool combined with full Excel functionality. Smart View enables you to interactively analyze your balances and define reports using a familiar spreadsheet environment. These queries are mainly for users in General Ledger. To share Smart View queries, users can email them to other users, or they can upload the queries to the Financial Reporting Center where users can

download them to a local drive for use. The Financial Reporting Center is only a place for users to upload and download Smart View queries.

> **Note:** To upload a Smart View report to the Financial Reporting Center: select the Open Workspace for Financial Reports task, navigate to the BI Catalog, and select **Upload** from the Tasks section. Be sure to upload the Excel file to one of the folder locations mentioned previously.

- Oracle Transactional Business Intelligence Analyses: These analyses and reports are built off of transactional tables using subject areas. These reports can be run by users in General Ledger, Payables, Receivables, Cash Management, Intercompany, and so on.
- Oracle Transactional Business Intelligence Dashboards: Dashboards put all the information, functions, and actions that a business user must have to do their job in one place. Dashboards are built off of Oracle Transactional Business Intelligence objects like analyses and reports. These reports can be run by users in General Ledger, Payables, Receivables, Cash Management, Intercompany, and so on.
- Oracle Analytics Publisher Reports: Most of these reports are predefined and must first be submitted and resubmitted to see the latest data by the Oracle Enterprise Scheduler through the Scheduled Processes navigation. These reports can be run by users in General Ledger, Payables, Receivables, Cash Management, Intercompany, and so on.
- BI Mobile Apps: Oracle Business Intelligence Mobile App Designer is an application that enables you to create multitouch information-driven applications with rich interaction, rich visualization, and rich media, for mobile devices such as iPhone, iPad, Android phone, tablet, and more. These reports can be run by users in General Ledger, Payables, Receivables, Cash Management, Intercompany, and so on.

Other Reporting Tools

Six other tools are available for reporting in Financials.

The following table lists the other reporting tools and the types of reports they support.

Other Reporting Tools	Report Type
General Accounting Dashboard and Account Inspector	Account Groups
Reports and Analytics	Oracle Transactional Business Intelligence Objects
BI Catalog	All Report Types, Except Oracle Analytics Publisher Reports
Enterprise Performance Management Workspace	Reports, Books, Snapshot Reports, Snapshot Books, Financial Reporting Batches, and Batch Scheduler
Enterprise Scheduler System	Oracle Analytics Publisher Reports

Even though the Financial Reporting Center is designed to be the main user interface for a financial end user's reporting needs, some users may choose to use any of the six other tools for reporting in financials, such as:

- General Accounting Dashboard, which provides access to Account Groups: Uses the Account Monitor to efficiently monitor and track key account balances in real time.

- Account Inspector: Perform ad hoc queries from account groups and financial reports through drill down to underlying journals and subledger transactions.
- Reports and Analytics: This reporting tool has a panel that reflects the folder structure of the BI Catalog. Users can access and run any Oracle Transactional Business Intelligence analysis, report or dashboard. Users can't run predefined Financial Reports or Oracle Analytics Publisher reports from this interface. This interface can be used by all financials users.
- BI Catalog: A component of the Enterprise Performance Management Workspace where you can run all report types, except for predefined Oracle Analytics Publisher reports.
- Enterprise Performance Management Workspace: Create reports, books, snapshot reports, snapshot books, Financial Reporting batches, and batch scheduler, and schedule batches to automatically run and burst to email.
- Enterprise Scheduler System: Only Oracle Analytics Publisher reports can be submitted from this interface. Users access this interface by navigating to **Tools** > **Scheduled Processes**. Most financial users have access to this interface to run standard reports for General Ledger, Payables, Receivables, and so on.

Related Topics

- Set Up Financial Reporting Center and Smart View
- How to Access EPM Narrative Reporting Reports in Financial Reporting Center

Create a Folder from the Financial Reporting Center

The Financial Reporting Center is a tool for accessing, designing, and presenting financial reports and analytic data.

Configure Financial Reporting Center

You have access to reports through the folder structure in the Financial Reporting Center and Workspace that's installed with Oracle Fusion Financials. Your Oracle Fusion Business Intelligence (BI) administrator defines the folder structure in Workspace your company's security requirements for folders and reports, as well as report distribution requirements for financial reporting batches.

Security can be set on folders and reports from Workspace. The BI Catalog stores both the Financial Reports and the BI Publisher Reports. Your BI administrator grants access to the folders and reports that you need.

Create and Secure a Folder Structure

To create a folder or subfolder:

1. From the Financial Reporting Center, open the Tasks pane and click the **Open Workspace for Financial Reports** task.
2. From the Navigate menu, select **Applications**, then **BI Catalog**.
3. On the Oracle BI Catalog page, go to the location in the Folders panel where you want to create the folder.
4. In the Oracle BI Catalog toolbar, click **New** and select **Folder**.
5. On the New Folder window, enter the folder name.
6. Click **OK**.

To assign permissions to a folder:

1. From the Financial Reporting Center, open the Tasks pane and click the **Open Workspace for Financial Reports** task.
2. From the Navigate menu, select **Applications**, then **BI Catalog**.
3. Search for the folder to which you want to assign permissions.
4. Go to the Tasks panel and click **Permissions**.
5. On the Permissions window, click the **Add user or roles** icon.
6. On the Add Application Roles and Users window, query the roles and select the ones you want to add.
7. Click the **Move** button.
8. Set the permission to the intended level, for example, **Full Control**.
9. Click **OK**.

Configure Smart View Client for Users

Smart View is a multidimensional pivot analysis tool combined with full Excel functionality. Smart View enables you to interactively analyze your balances and define report using a familiar spreadsheet environment.

Install Smart View, an add-in to Excel, to each client computer. To download the installation files:

1. Navigate to the Financial Reporting Center and select the **Open Workspace for Financial Reports** task.
2. In the Enterprise Performance Management System Workspace, select **Tools** > **Install** > **Smart View**.

> **Note:** Because Smart View is an add-in to Microsoft Office products, you can install Smart View only on a Windows operating system.

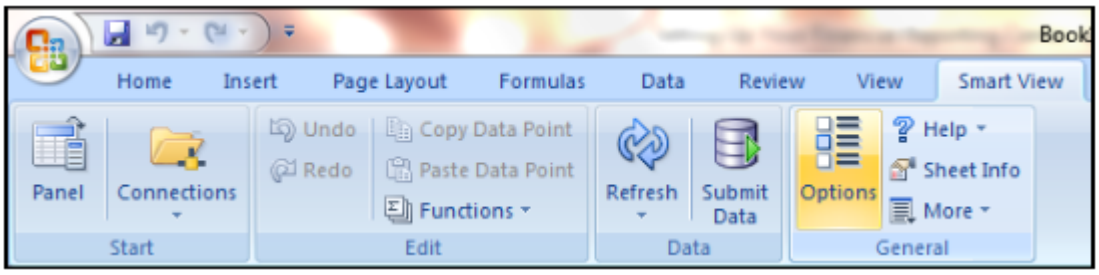
Once Smart View is installed, you must configure the connection using the Smart View Shared Connections URL. To derive the Shared Connections URL follow these steps:

1. From the Financial Reporting Center task panel, select **Open Workspace for Financial Reporting**.
2. Edit the workspace URL by removing **index.jsp** and adding **SmartViewProviders** at the end.

   > **Note:** For example, if the workspace URL is **https://example.com/workspace/index.jsp**, the shared connections URL would be **https://example.com/workspace/SmartViewProviders**.

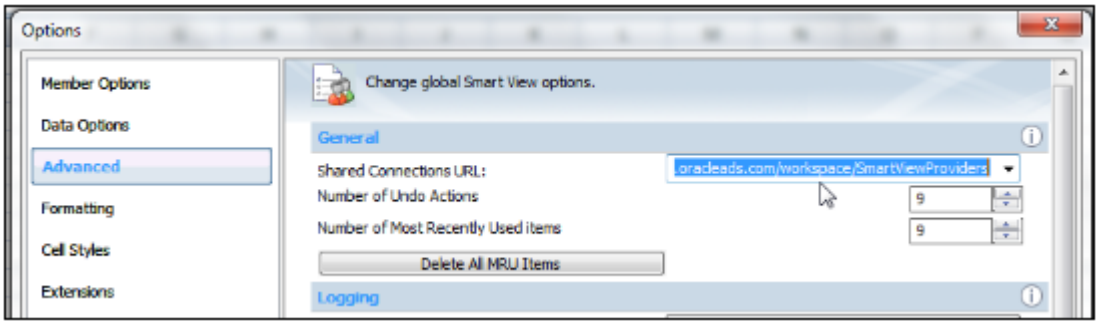
3. Copy the URL.
4. Open Excel.
5. Navigate to the **Smart View** menu > **Options**

   This image shows the Smart View ribbon on the Excel spreadsheet. The task lists include Panel, Connections, and Options.



6. Click the **Options** button and select the **Advanced** option.

   The following figure shows the Options window with the Advanced option selected. The shared connections URL appears in the General section.



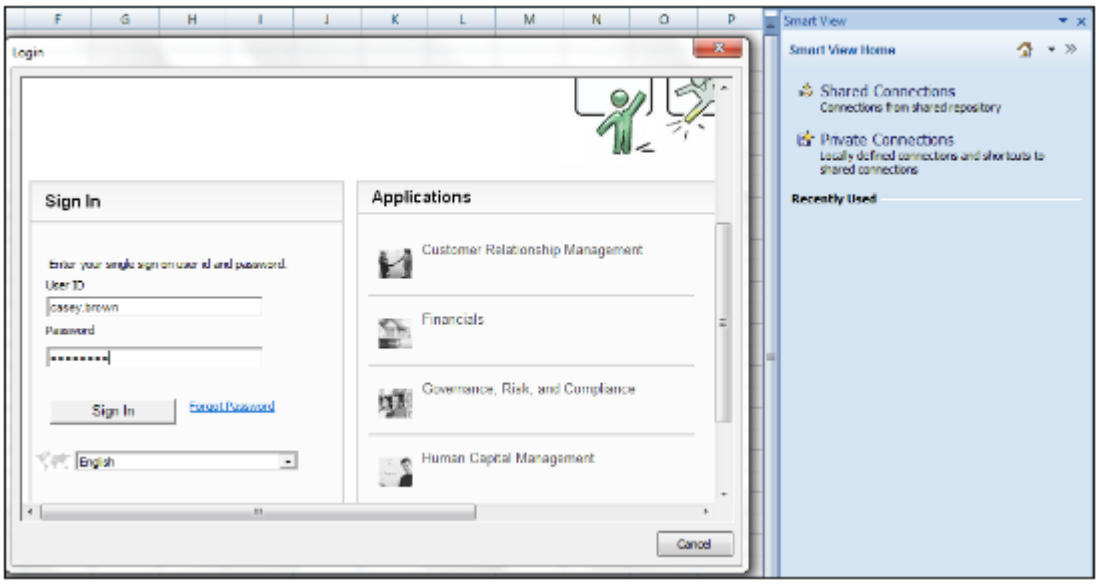
7. Paste the URL in the **Shared Connections URL** field.
8. Click **OK**.

For more information about configuring the Smart View client for users, see the Oracle Smart View for Office User's Guide.

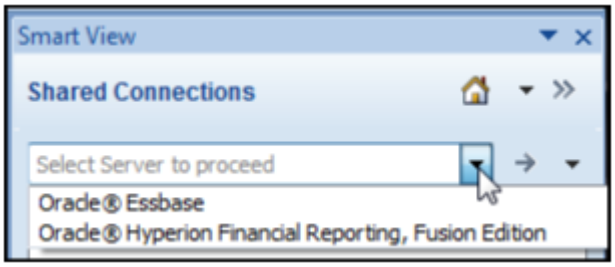
To connect to Oracle Fusion General Ledger Balances cubes in Smart View:

1. Start Smart View.
2. Click the Smart View tab and select the **Panel** icon. The Smart View pane opens.
3. Click the **Shared Connections** button on the task pane.
4. Sign in with your user name and password.

   The following image shows the Sign In window for connecting to the database.



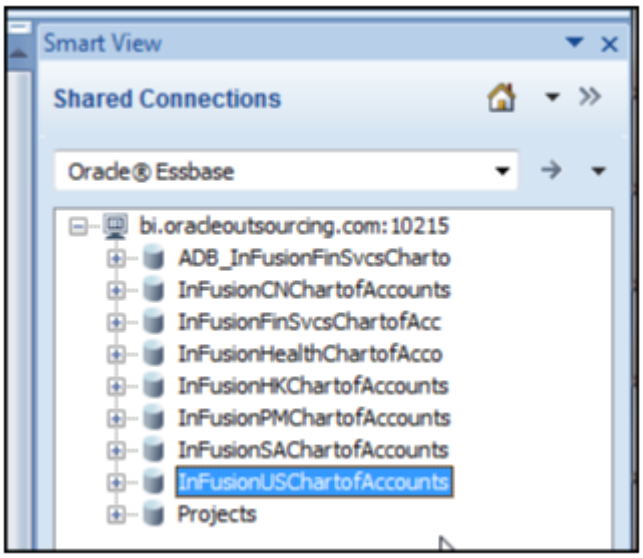
5. Click the **Select Server** list icon to proceed.
   The following figure shows the Shared Connections section on the Smart View panel. The Select Server to proceed field is selected and two values appear in the drop-down list: Oracle Essbase, Oracle Hyperion Financial Reporting.



   Note: If the Essbase Server isn't there, then it must be added. Use the following steps:

   a. Click the **Add Essbase Server** link.
   b. Specify the Essbase Server login and password.
   c. Expand the Essbase server and find its cube.

6. Select Oracle Essbase from the list of shared connections.
7. Click the **Expand** to expand the list of cubes.
8. Expand your cube that has the name of your chart of accounts.
   The following figure shows the Shared Connections section on the Smart View panel. The Oracle Essbase server is expanded, showing several cubes.



9. Click db. A list of functions appears.
10. Click the analysis link.

Note: You must perform these steps only once for a new server and database.

To set how the name and alias of the Essbase database appears:

1. On the Smart View ribbon, click the **Options** button.
2. Select **Member Options** from the list and select the **Member Name Display** list.

3. You can select from among the following options:
   - Distinct Member Name: Only shows the full Essbase distinct path.
   - Member Name and Alias: Shows both the member name and the alias.
   - Member Name Only: Shows only the member name.

Note: The Smart Slice feature isn't supported in General Ledger. For all other documentation, see the Oracle Smart View for Office User's Guide.

Define Database Connections in Workspace for Financial Reports

You must create database connections so you can access the cubes from Workspace and Financial Reporting Web Studio.

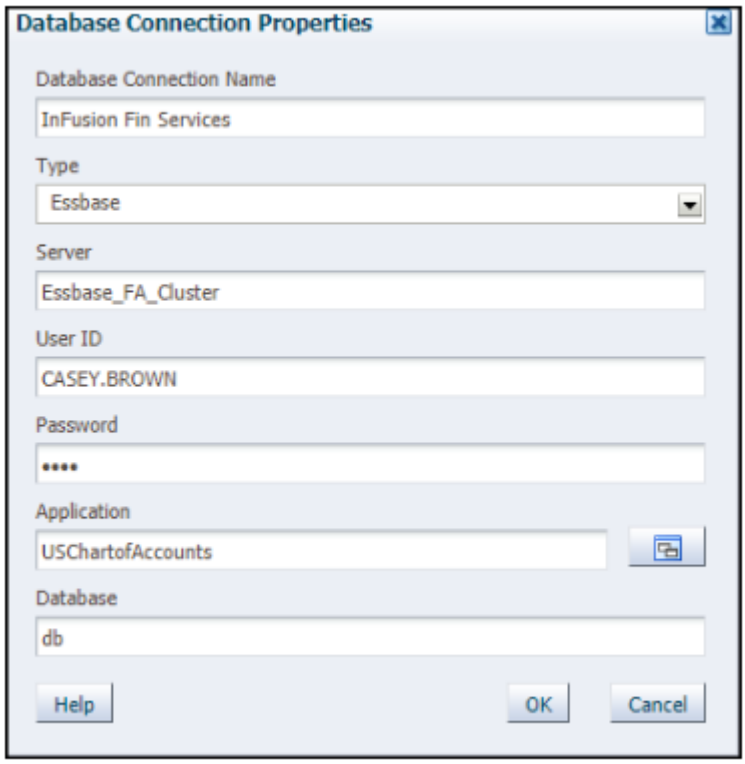
Note: Ledger setup has to be completed before the database connection can be created. Oracle Fusion General Ledger balances cubes are created as part of ledger setup. Each combination of chart of accounts and accounting calendar has a separate cube. Each cube needs a database connection.

Steps to define a database connection are:

1. From the Financial Reporting Center work area, open the Tasks panel and select the **Open Workspace for Financial Reports** task.
2. From within the workspace, select the **Navigate** menu > **Applications** > **BI Catalog**.
3. From the **Tools** menu, select **Database Connection Manager**.
4. On the Database Connection Manager window, click **New**.
5. Enter a user-friendly name for the database connection name.
6. Enter Essbase as the **Type**, your server, user name, and password.
7. Select **Application** (cube) and **Database** from the list of values.

8. Expand the **Application** name to see the related database, for example, db.

   The following figure shows the Database Connection Properties window with the completed fields from steps 5 through 8.



9. Click **OK** twice to save your selections.
10. Click **Close** to save the connection.

For more information about configuring Essbase database connections in Workspace see: **Oracle Essbase Database Administrator's Guide**.

> **Note:** The database connection is available in both Workspace and Financial Reporting Web Studio. Optionally, the database connection can be set up in Financial Reporting Web Studio while entering the grids on a report.

Create a Financial Report

Define a Basic Financial Report Using the Reporting Web Studio

This is the first of six topics on designing a financial report with Financial Reporting Web Studio.

Watch video

You can use Financial Reporting Web Studio to design traditional financial report formats such as balance sheets, profit and loss statements, and cash flow reports. You can also design nontraditional reports for financial or analytic data that include text and graphics.

In this example, you're designing a basic financial report.

1. From the Financial Reporting Center work area, select the Tasks panel tab and click **Open Workspace for Financial Reports**.
2. On the **Tools** menu, select **Launch Financial Reporting Web Studio**.
3. On the **File** menu, select **New**, **Report**.
4. On the toolbar, click the **Grid** icon. Grids are tables that contain data from external database connections.
5. In the design canvas, draw a box to create the grid. The Database Connection Properties dialog box opens.

   > **Tip:** When creating a grid, best practice is to leave space in the design canvas for other objects, such as a company logo and report title.

6. Select the **Data Sources** list and select the data source for the chart of accounts that the report is based on. A unique cube exists for each combination of chart of accounts and accounting calendar.

   > **Tip:** Best practice is to always turn on suppression in financial reports at the Database Connection Server level. You can verify the setting by highlighting the grid, and then selecting **Data Query Optimization Settings** on the **Task** menu. For most reports, best practice is to turn on suppression for the entire grid. Then turn suppression off for columns and rows that must always display. For more information about suppression settings, refer to the Defining Basic Conditional Suppression section in the Financial Reporting Web Studio User's guide.

7. Click **OK**. The Dimension Layout dialog box opens.

Arrange the Dimensions

Use the Dimension Layout dialog box to arrange the dimensions on your report. For this report, the accounting periods display on the columns and the revenue and expense account information displays on the rows. The company appears on each page and can be selected at runtime.

1. Drag the **Accounting Period** dimension to the **Columns** axis.
2. Drag the **Account** dimension to the **Rows** axis.
3. Drag the **Company** dimension to the **Page** axis.
4. Click **OK** to close the Dimension Layout dialog box.

Define the Rows

Use the Select Members dialog box to define the revenue and expense account rows.

1. Select the revenue parent account.
   a. Double-click the **Account** cell. The Select Members dialog box opens with a default member selected.
   b. Remove the default **Account** selection from the Selected area by clicking it to select it and then clicking the **Remove from Selected** icon.
   c. In the **Search** field, enter the value for the account that represents total revenue and click the **Search** icon.
   d. Select the account from the search results and click **OK**. The account moves to the Selected area.
   e. Click **OK**. The Select Members dialog box closes.
2. Now insert a text row to add space between the revenue and expense accounts.

a. Select the last row in the grid by clicking the row header.
b. On the **Insert** menu, select **Row**, then **Text**.

3. Insert a row for the expense accounts.
   a. Right-click the last row header.
   b. On the **Insert Row** menu, select **Data**. Notice the default value for the new row is the revenue parent account.
4. Select the expense parent accounts.
   a. Double-click the account value in the new expense account row. The Select Members dialog box opens with the revenue parent account selected.
   b. Remove the revenue parent account selection from the Selected area by clicking to select it and then clicking the **Remove from Selected** icon.
   c. In the Available area, expand the **Account** member, and continue expanding until you find the expense parent accounts for the report.
   d. Select the accounts and click the **Add to Selected** icon to move them to the Selected area.
   e. Select the **Place selections into separate rows** option so each account appears in its own row on the report.
   f. Click **OK**. The Select Members dialog box closes.

Save and Preview the Report

Save the report and leave it open for the next topic, which is adding a formula to a financial report.

1. Click the **Save** icon.
2. Select the folder with your name and enter the report name and description.
3. Click **Save**.
4. Optionally preview the report in HTML or PDF format using the **File** menu or toolbar.

Add Formulas to a Financial Reporting Report

This is the second of six topics on designing a financial report with Financial Reporting Web Studio.

Watch video

In this example, you define a formula to summarize the expense account balances on your financial report.

Before you start, do the steps described in the Define a Basic Financial Report Using the Reporting Web Studio topic, then follow these steps.

1. Right-click the last row header, select **Insert Row** and select **Formula**.
2. Click in the empty cell in the new row.
3. In the Heading Row Properties pane, select the **Custom Heading** option, enter **Total Expenses** and click the **Update** icon. The new heading appears in the report.
4. Select the row header for the formula row. The SUM function appears in the design canvas.
5. In the Formula bar, click the **Sum(0)** button and enter the formula and cell references in the formula text box. Because the expense rows appear one after the other, you can use the first row number and the last row number with a colon in between. For example, Sum([3:5]). If the rows weren't contiguous, you could put brackets around each row number and separate them with commas. For example, Sum([3], [5], [6]).

6. Validate the formula syntax by clicking the check mark icon in the toolbar. Validation checks the validity of the formula, not if the data is available.
7. Save the report and leave it open for the next topic, which is defining a range function. Optionally preview the report.

Define Range Functions for a Financial Reporting Report

This is the third of six topics on designing a financial report with Financial Reporting Web Studio.

Watch video

In this example, you define a range function to report across multiple accounting periods. You configure the range to present balances for the last 12 months from the period selected at runtime.

Before you start, do the steps described in these topics.

1. Define a Basic Financial Report Using the Reporting Web Studio
2. Add Formulas to a Financial Reporting Report

Now follow these steps.

1. Double-click the **Accounting Period** cell. The Select Members dialog box opens.
2. Remove the default accounting period from the Selected area by clicking it to select it and then clicking the **Remove from Selected** icon.
3. Click the Functions tab.
4. Select **Range** from the list.
5. Click the **Add to Selected** icon. The Range dialog box opens.
6. Define the starting member for the range.
    a. On the Start Member row, click the **Lookup Selection** icon in the **Value** column.
    b. Click the Functions tab.
    c. Select the **Relative Member** function to define the periods that display on the report relative to the period specified at runtime.
    d. Click **OK**. The Relative Member dialog box opens.
    e. On the Member row, click the **Lookup Selection** icon in the **Value** column.
    f. Select **Current Point of View for Accounting Period** so you can enter the starting period for the report.
    g. Click **OK**.
    h. On the Offset row, enter -11 in the **Value** field.

        The offset determines the first period of the range. The starting period in the range function is always the oldest period. Because this is a rolling 12 period report, enter -11 to include the 11 periods prior to the period you enter at runtime. The member selection for the End Member parameter determines period 12.
    i. Click **OK**.
7. Define the ending member for the range.
    a. On the End Member row, click the **Lookup Selection** icon in the **Value** column.
    b. Select **Current Point of View for Accounting Period**.
    c. Click **OK**.
    d. Click **OK** to close the Range dialog box.
    e. Click **OK** to close the Select Members dialog box.

8. Save the report and leave it open for the next topic, which is defining a grid point of view. Optionally preview the report.

Set User and Grid Points of View for a Financial Reporting Report

This is the fourth of six topics on designing a financial report with Financial Reporting Web Studio.

Watch video

In this example, you set a user point of view and a grid point of view for a financial report.

All financial reporting reports have a user point of view and a grid point of view. Best practice is to use a combination of both.

If you want users to select certain dimension members at runtime, then those dimensions should be set in the user point of view. Selections for user point of view members are global for a user and data source. This means the application saves and applies them to any other report that has the same dimensions set to the user point of view. By default, all dimensions are set to the user point of view and must be selected at runtime. If you want your report to always use certain dimension selections, then select the specific members in the grid point of view.

Note: Members of a grid point of view only display in HTML.

In this example you set the Ledger, Scenario, Balance Amount and Currency dimensions to use the grid point of view.

Before you start, do the steps described in these topics.

1. Define a Basic Financial Report Using the Reporting Web Studio
2. Add Formulas to a Financial Reporting Report
3. Define Range Functions for a Financial Reporting Report

Now follow these steps.

1. Select the cell in the grid that represents the intersection of the rows and columns. The Grid Properties pane opens.
2. In the Grid Properties pane, click the **Grid Point of View** check box.
3. In the design canvas, click the **Ledger**: **User Point of View for Ledger** button. The Select Members dialog box opens.
4. Expand the **Ledger** member and continue to expand until you find the ledger to include on the report. Select the ledger.
5. Click **Apply Selection**.
6. Select **Scenario** from the Dimension list to select the type of balance to use on the report.
7. Expand the **Scenario** member and select **Actual**.
8. Click **Apply Selection**.
9. Select **Balance Amount** from the Dimension list.
10. Expand the **Balance Amount** member and select **Period Activity**.
11. Click **Apply Selection**.
12. Select **Currency** from the Dimension list.
13. Search for **USD**.
14. Click **OK** to accept the search result.
15. Click **Apply Selection**.
16. Click **OK** to close the Select Members dialog box.

17. Save the report and leave it open for the next topic, which is setting page and grid properties. Optionally, preview the report.

Work with Grid Point of View Setup and Page Axis for a Financial Reporting Report

This is the fifth of six topics on designing a financial report with Financial Reporting Web Studio.

Watch video

In this example, you change the grid point of view setup and set the page member selection to a prompt on your financial report.

Before you start, do the tasks described in these topics.

1. Define a Basic Financial Report Using the Reporting Web Studio
2. Add Formulas to a Financial Reporting Report
3. Define Range Functions for a Financial Reporting Report
4. Set User and Grid Points of View for a Financial Reporting Report

Now follow these steps.

1. Click the first cell in the grid to select all of the rows and columns.
2. Right-click and select **Grid Point of View Setup** from the list. The Setup Grid Point of View dialog box opens.
    a. To prevent the **Balance Amount** dimension from being changed at runtime, select the **Lock Member Selection** option.
    b. Click **OK**. The Setup Grid Point of View window closes.
3. In the Grid Properties pane:
    a. Click the **Drill Through** option to allow drilling from the report to the General Ledger transaction data.
    b. Click the **Suppression** section to view the suppression settings.
    c. Enter 0 in the **Zero Values** field to set the text option for rows with zero values. If necessary, you could also suppress the display of rows with zero values, rows with missing data, and rows with errors.
4. Set a runtime prompt for the Company dimension so you have the flexibility of selecting any company or combination of companies at runtime. In this example, you want to restrict the valid list of companies that can be selected at runtime.
    a. On the grid, click the **Pages** label. The Company dimension appears in the design canvas.
    b. Click the **Company** button. The Select Members dialog box opens.
    c. Remove the default **Company** selection from the Selected area by clicking it to select it and then clicking the **Remove from Selected** icon.
    d. Select **Prompt for Company**.
    e. Click the **Add to Selected** icon to move the selection to the Selected area.
    f. Click **OK**. The Define Prompts dialog box opens.
    g. Click the **Lookup** icon in the **Choices List** field. The Select Members dialog box opens.
    h. Remove the default **Company** selection from the Selected area by clicking it to select it and then clicking the **Remove from Selected** icon.
    i. Expand the Company member, and continue expanding until you find and select the default companies you want to display in the prompt.

j. Click the **Add to Selected** icon to move the companies to the Selected area.
k. Click **OK**. The Select Members window closes.
l. On the Define Prompts dialog box, click in the **Member Name** field and select **Alias**. The actual company label displays in the prompt list of values instead of a numeric company value, making the prompt more user-friendly.
m. Click **OK**. The Define Prompts window closes.

5. Click the **Pages** label on the grid. The Page Properties pane opens.
   a. In the Page Properties pane, select the **Alias**: **Default** option so each page of the report shows the name of the company instead of the number.
6. Select the four data rows in the grid so all of the rows have the same settings.
   a. In the Heading Row Properties pane, select the **Alias**: **Default** option in the Heading Row Properties pane to display the revenue and expense account names instead of the accounts.
   b. In the Heading Row Properties pane, select the **Allow Expansion** option so you can expand the parent account values to view the detail child values.
7. Save the report and leave it open for the next topic, which is formatting your financial report and adding a graph. Optionally, preview the report.

Add Formats and Graphs to a Financial Reporting Report

This is the sixth and final topic in a series of topics on designing a financial report with Financial Reporting Web Studio.

Watch video

In this example, you add formats and graphs to a financial report.

Before you start, do the steps described in these topics.

1. Define a Basic Financial Report Using the Reporting Web Studio
2. Add Formulas to a Financial Reporting Report
3. Define Range Functions for a Financial Reporting Report
4. Set User and Grid Points of View for a Financial Reporting Report
5. Work with Grid Point of View Setup and Page Axis for a Financial Reporting Report

Now follow these steps.

1. In the report object browser, select the name of the report, which is the first object.
2. Add a logo.
   a. In the report layout, drag the header line to make space for the logo and title.
   b. In the Header section, click the **Add Report Object** icon and select **Image**.
   c. In the Image Properties pane, click **Browse** and select your company logo.
3. Add a title.
   a. Select the name of the report in the report object browser.
   b. In the Header section, click the **Add Report Object** and select **Text**. As an alternative, you can click the **Text** icon in the toolbar and draw the text box. The text box opens.
   c. Enter the report title.
   d. Select the title text and use the format toolbar to adjust the font size, center the text, and change the font style to bold.

4. Change the page orientation.
    a. Select the name of the report in the report object browser.
    b. On the **File**, menu, select **Page Setup**.
    c. In the Page Setup dialog box, select the **Landscape** option.
    d. Click **OK**.
5. Add a chart.
    a. In the Body section, click the **Add Report Object** icon and select **Chart**.
    b. In the Chart Properties pane, select the **Line** chart type.
    c. To show only the expense account rows, deselect row 1, and select rows 3, 4, and 5 in the Data Range section.
    d. Click the **Format Chart** button. The Format Chart dialog box opens.
    e. In the Appearance tab, enter the title for the chart. For example, **Expenses by Period**.
    f. Click the Legend tab and enter a title for the legend. For example, **Type of Expenses**.
    g. Click the Axes tab and enter a title for the Metadata axis. For example, **Period**. Enter a title for the Primary Axis. For example, **Dollars**.
    h. Click the **Refresh Chart** button to preview the chart on the Format Chart dialog box.
    i. Click **OK**. The Format Chart dialog box closes.
6. Save the report and optionally, preview it.

For more information about Financial Reporting Web Studio, select the Using EPM with Oracle Financials Cloud link from the All Books for Oracle Financials Cloud page of the Oracle Help Center at https://docs.oracle.com.

5 Implement AI Apps for Financials

AI Apps Implementation Workflow

Follow these high-level steps to get started with AI Apps for Financials. See the sections in this chapter to get more detailed implementation instructions where you need them.

Before you start

Before implementing AI Apps for Financials, make sure that the Cloud ERP environment for your organization meets this criteria:

- Must not be deployed on a US Government Cloud pod
- Should be live in production with at least 3 months of consumable data to benefit from high quality recommendations and prediction results

Step 1: Create users and assign roles

Create the users and roles in Oracle Cloud Financials to enable communication and data exchange for AI Apps and schedule and run the data extracts in Oracle BI Publisher. Create the user to access the administrator tasks in AI Apps for ERP.

Step 2: Set up AI Apps

On the Connections page in Oracle AI Apps for ERP, make the connections for your integrations with your Oracle Financials service.

Step 3: Opt in for AI Apps for Financials features

In the Setup and Maintenance work area of Oracle Financials, enable the applicable features.

To understand AI Apps features and setting them up, watch this video:

- *Intelligent Account Combination Defaulting Setup Instructions*

Create Users and Assign Roles

Create AI Apps Admin Users

Admin users who can access AI Apps for ERP for initial setup and ongoing management of connections and supervisory controls, must have the Application Implementation Consultant role. Your IT security manager can assign this role from the security console in your Oracle Financials Cloud environment.

Create the Business Intelligence User and Role

The AIAPPS_BIP_ROLE role is required in Oracle Business Intelligence (BI) to extract values from Oracle Financials Cloud and train the AI Apps machine-learning models.

> **Note:** It's best practice to create a dedicated user, however, you may prefer to create and add this role to an existing user. To avoid any disruption of the services, ensure that this user is excluded from password reset policies.

1. Connect to the Oracle Financials Cloud as a user with the IT Security Manager role.
2. In the Navigator menu, under **Tools**, click **Security Console**. You may need to click **More** to expose the Tools options.
3. Create the AIAPPS_BIP_ROLE:
    a. On the Roles page, click **Create Role**.
    b. Enter these values:

Field	Value
Role Name	AIAPPS_BIP_ROLE
Role Code	AIAPPS_BIP_ROLE
Role Category	BI - Abstract Roles

    c. Click **Next** three times.
    d. On the Role Hierarchy stop, click **Add Role**.
    e. In the Add Role Membership window, search for and select **BIAuthor**, then click **Add Role Membership**.
    f. Search for and select **BIPDataModelDeveloper**, then click **Add Role Membership**.
    g. Click **Cancel** to close the window.
    h. Click **Next** two times.
    i. Click **Save and Close**, and then click **OK**.
4. Create a user account named AIAPPS_BIP with the AIAPPS_BIP_ROLE role:
    a. Click **Users**.
    b. On the User Accounts page, click **Add User Account**.
    c. In the User Information section, enter values for all of the required fields.
    d. Rename the User Name value to **AIAPPS_BIP**.
    e. Click **Add Role**.
    f. In the Add Role Membership window, search for and select **AIAPPS_BIP_ROLE**, then click **Add Role Membership**.
    g. Click **Done** to close the window.
    h. Click **Save and Close**.

5. Schedule a process to import the user and role security data as follows:
    a. From the Navigator menu, in the Tools section, select **Scheduled Processes**.
    You may need to click **More** to expose the Tools options.
    b. Click **Schedule New Process** and select the values shown here:

Field	Value
Type	Job
Name	Import User and Role Application Security Data

    c. Click **OK**.
    d. In the Process Details window, click **Submit**.
    e. Make a note of the process ID, and then click **OK**.
    f. Click **Refresh** until the status of the process ID you noted shows as succeeded.

Set Up AI Apps

Connect AI Apps to Business Intelligence

To ingest data for AI model training and supplier categorization with Oracle BI Publisher, you must connect using the appropriate credentials.

1. Sign in to AI Apps for ERP as a user with the Application Implementation Consultant role.
To access the AI Apps for ERP application:
    a. If you're not already on the Home page, click the company logo in the page header.
    b. Use the arrow in the tab carousel to scroll, and click the Tools tab.
    c. In the Quick Actions section, click **AI Apps Administration**.
    This will open the AI Apps Administration UI in a separate browser tab.
    d. Select **AI Apps for ERP**.
    This will open the AI Apps for ERP UI in a separate browser tab. You can bookmark this page to directly access the applications in the future.
2. Click **Connections**.
3. In the Oracle Business Intelligence section, click **Edit**.
4. Enter these values:

Field	Value
User Name	The user name you created for the Business Intelligence user. For example AIAPPS_BIP.

Field	Value
Password	The password associated with that user name. **Note:** If you change the password later, you must also update it here. The passwords must match.

5. Click **Save**.

After the Oracle Business Intelligence section is completed and saved, the data ingestion and model training will begin. You can expect to have a working model for AI Apps features after 8 to 12 hours, depending on the volume of data. Some large data sets may require more time. Check the Oracle Data Science section on the Connections page to view the status of the training. For details, see *Train Models for AI Apps Features and Download Evaluation Reports*.

Related Topics

- Create the Business Intelligence User and Role

Train Models for AI Apps Features and Download Evaluation Reports

AI Apps uses machine learning models with algorithms that are trained and optimized on your data. Without creating large volumes of test data, you can understand the potential performance of an AI Apps feature using the model evaluation report.

For a model evaluation report, you need to connect AI Apps to Business Intelligence and train the model. After it's trained, you can download the evaluation report. Here's how you can do that:

1. Sign in to AI Apps for ERP as a user with the Application Implementation Consultant role.

   To access the AI Apps for ERP application:

   a. If you're not already on the Home page, click the company logo in the page header.
   b. Use the arrow in the tab carousel to scroll, and click the Tools tab.
   c. In the Quick Actions section, click **AI Apps Administration**.

      This will open the AI Apps Administration UI in a separate browser tab.
   d. Select **AI Apps for ERP**.

      This will open the AI Apps for ERP UI in a separate browser tab. You can bookmark this page to directly access the applications in the future.
2. Click **Connections**.
3. Verify that AI Apps is connected to Business Intelligence. If it's not, connect now. For details, see *Connect AI Apps to Business Intelligence*.

4. If you're setting up a nonproduction environment to train an AI model, enter the latest P2T refresh date to replace your existing training data with the data that's been in production up to the refresh date.
    a. In the P2T refresh section, click **Edit**.
    b. In the P2T Refresh window, **Latest P2T Refresh Date** field, select the latest date that the connected tenant was refreshed from production.
    c. Click **Update Training Data**.

    The AI model will now be trained on the latest data copied from production. This ensures that there's enough and relevant data to train the model and generate the evaluation report.

    In the Oracle Data Science section, you can view the status of the model training for the feature.
5. After the model training is complete, click **Download Report** for the feature.

Use the report to understand the potential performance of the feature on your data. In the evaluation report for the Intelligent Account Combination Defaulting feature, you can find the promotion code to opt in to the feature.

Opt In for AI Features

Opt In for Intelligent Account Combination Defaulting

The entry of a promotion code is required to display this feature as an option that you can select within the Setup and Maintenance area of your Oracle Cloud ERP environment. After you enter the promotion code, you can turn this feature on or off within your environment.

You can find the promotion code in the evaluation report that's generated after data ingestion and model training. For details, see *Train Models for AI Apps Features and Download Evaluation Reports*.

1. Sign in to Oracle Financials Cloud as a user with the Application Implementation Consultant role.
2. To enter the promotion code, follow these steps:
    a. On the Navigation menu, select **My Enterprise** > **Enterprise**.
    b. Click **Manage Promotions Codes**.
    c. Click **Enter Promotion Code**.
    d. Enter your promotion code and click **Save and Close**.
    e. Check that your code is displayed as Intelligent Account Combination Defaulting for Invoices Promotion Code. If it isn't displayed so, contact your Oracle representative.
3. On the Navigation menu, select **My Enterprise** > **Setup and Maintenance**.
4. On the Setup list in the page header, select **Financials**.
5. Click **Change Feature Opt In**.
6. If not already expanded, expand **Financials**, and then expand **Supplier Invoice Processing**.
7. Select the **Payables** row, and then click the Features edit icon.
8. Select the row for the feature named Intelligent Account Combination Defaulting for Invoices, then click the **Enable** box in that row.
9. Click **Save and Close**, and then click **Done**.
10. Click **Done** again to return to the Financials setup page.

Predictions will be served after you opt in to.

6 Rapid Implementation Spreadsheets

Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheets

Represent your enterprise structures in your chart of accounts, ledger, legal entities, and business unit configuration to track and report on financial objectives and meet reporting requirements. These components provide the underlying structure for organizing financial information and reporting.

The chart of accounts within the ledger facilitates:

- Aggregating data from different operations, from within an operation, and from different business flows
- Consistent definitions to your stakeholders in compliance with legislative and corporate reporting standards and aids in management decisions

Rapid implementation is a way to configure a financial enterprise and financial reporting structures quickly using sheets in a workbook that upload lists of:

- Companies (legal entities)
- Ledgers by country
- Business units
- Chart of accounts and segment values
- Segment value hierarchies
- Financial sequences
- Required subledger accounts

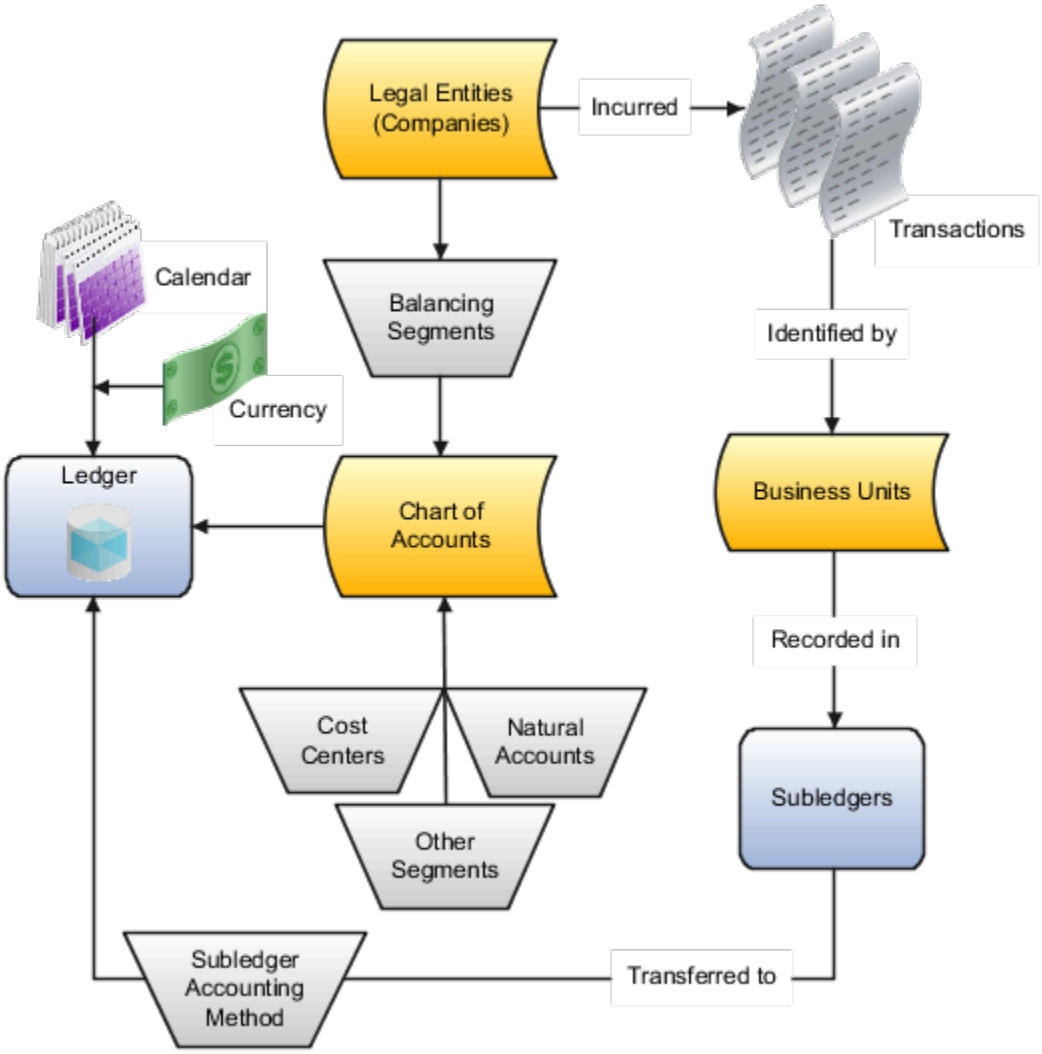
Once the sheets have been uploaded, the application creates:

- Chart of accounts structure and instance
- Segment value hierarchies
- Key accounts such as retained earnings
- Required subledger accounts
- Accounting calendar
- Primary ledger for each country represented on the legal entities sheet
- Legal entities and their locations
- Business units
- Document and journal sequencing
- Set of Financial Reporting reports
- Three account groups

CAUTION: Once you begin using your chart of accounts, calendar, and ledger, making changes to their fundamental attributes is neither recommended nor supported. This includes your chart of account segments, including the segment labels as well as other characteristics of those segments, and your calendar structure or pattern.

The following figure illustrates the flow of the enterprise structure setup.

Legal entities (companies) incur transactions that are identified by business units with business functions. Transactions that are recorded in subledgers are transferred to the ledger. A ledger is characterized by a calendar, a currency, and a chart of accounts. A chart of accounts consists of segments, some of which are assigned segment labels, such as cost center, natural account, and primary balancing segment. Legal entities can be assigned primary balancing segment values.



Additional information for some of the common setup objects depicted in the figure follows:

- **Legal Entity**: Identifies a recognized party with rights and responsibilities given by legislation, which has the right to own property and the responsibility to account for itself.
- **Business Units**: Performs one or many business functions that can be rolled up in a management hierarchy. A business unit can process transactions on behalf of many legal entities. Usually a business unit has a manager, strategic objectives, a level of autonomy, and responsibility for its profit and loss. When created through the spreadsheet, all available business functions are automatically enabled for the business unit.

- **Ledger**: Maintains records and is a required component in your configuration. The rapid implementation process:
    - Creates primary ledgers by combining the chart of accounts, calendar, and currency as well as other required options defined in the rapid implementation workbook.
    - Assigns the standard accrual subledger accounting method to the primary ledger. The subledger accounting method is used to group subledger journal entry rule sets together to define a consistent accounting treatment.
    - Creates a General Ledger balances cube for each ledger with a unique chart of accounts and calendar combination. Each segment is created as a dimension in the balances cube along with the standard cube dimensions.
- **Subledger**: Captures detailed transactional information, such as supplier invoices, customer payments, and asset acquisitions. Uses subledger accounting to transfer transactional balances to the ledger where they're posted.
- **Chart of Accounts**: Configures accounts that consist of components called segments. Accounts are used to record balances and organize financial information and reporting.
- **Segment**: Identifies one of the components of a chart of accounts, which when combined with other segments, creates an account combination for recording transactions and journal entries. A segment is associated with a value set, which provides the set of values for that segment, along with the formatting and validation for those values.
- **Segment Label**: Identifies certain segments in a chart of accounts and assigns special functionality to those segments.
    - **Balancing Segment**: Ensures that all journals balance for each balancing segment value or combination of multiple balancing segment values for financial processes and reports. The three balancing segment labels are: Primary Balancing Segment, Second Balancing Segment, and Third Balancing Segment.
    - **Natural Account**: Determines the account type (asset, liability, expense, revenue, or equity) and specific categorization of the financial activity. Facilitates General Ledger processes, such as closing of the income statement accounts to retained earnings at the beginning of a new fiscal year.
    - **Cost Center**: Facilitates grouping of natural accounts by functional cost types, accommodating tracking of specific business expenses across natural accounts.

With the rapid implementation workbook you can also:

- Create more than one hierarchy for any of your chart of accounts segments during initial setup. You can also create additional hierarchies and hierarchy versions, as well as update existing hierarchy versions, after the initial setup is done by uploading the rapid implementation spreadsheet data.
- Create sequences for each legal entity or ledger based on the predefined country defaults. Document sequences are created for: Payables invoices, Payments, Receivables invoices, Receivables credit memos, Receivables adjustment activities. Reporting and accounting journal sequences are created for subledger journals and General Ledger journals.

Related Topics

- How Charts of Accounts, Ledgers, Legal Entities, and Business Units Are Created Using Spreadsheets

How Charts of Accounts, Ledgers, Legal Entities, and Business Units Are Created Using Spreadsheets

The rapid implementation process for setting up an enterprise structure includes several steps.

1. Downloading the Rapid Implementation for General Ledger workbook.
2. Entering data into the sheets.
3. Verifying the entered data and resolving any errors.
4. Uploading the chart of accounts file.
5. After successful upload of the chart of accounts file, uploading the general ledger, legal entity, and business unit file with the rest of the configuration.

The rapid implementation enterprise structure configuration is meant to be used as a one-time initialization. To the extent that you want to make certain allowed modifications to the configuration, you generally have to make those changes directly in the applications. After initial upload of the ledger, legal entity, and business unit file, the fundamental accounting configuration framework is only created once and is permanently set. This framework includes the ledger and its assigned chart of accounts, calendar and currency assignment, and the associated definitions of those components.

Workbook Overview

You can download the workbook in one of two ways:

1. In the Setup and Maintenance work area, go to the **Manage Chart of Accounts Configurations** task in the Financial Reporting Structures functional area and click the **Download Setup Template** button.
2. In the Setup and Maintenance work area, create an implementation project that includes the **Define Financials Configuration for Rapid Implementation** task list. Download the workbook using the Create Chart of Accounts, Ledger, Legal Entities, and Business Units in Spreadsheet task.

The workbook includes the following sheets:

- Instructions
- Chart of Accounts, Calendar, and Ledger
- Business Units
- Companies and Legal Entities
- Natural Accounts
- Financial Sequences

New sheets for entering segment values and hierarchies for additional segments of your chart of accounts can be created automatically. After you enter the segments on the Chart of Accounts, Calendar, and Ledger sheet, click **Add Segment Sheets** or **Generate Additional Hierarchy**.

> **Note:** The rapid implementation process creates a standard ledger. You can convert a standard ledger to an average daily balance ledger before the first period is opened by selecting the **Enable average balances** check box on the Specify Ledger Options page.

Instructions

Review the Instructions sheet for important information about how to use the workbook and submit the accounting configuration. The sheet includes:

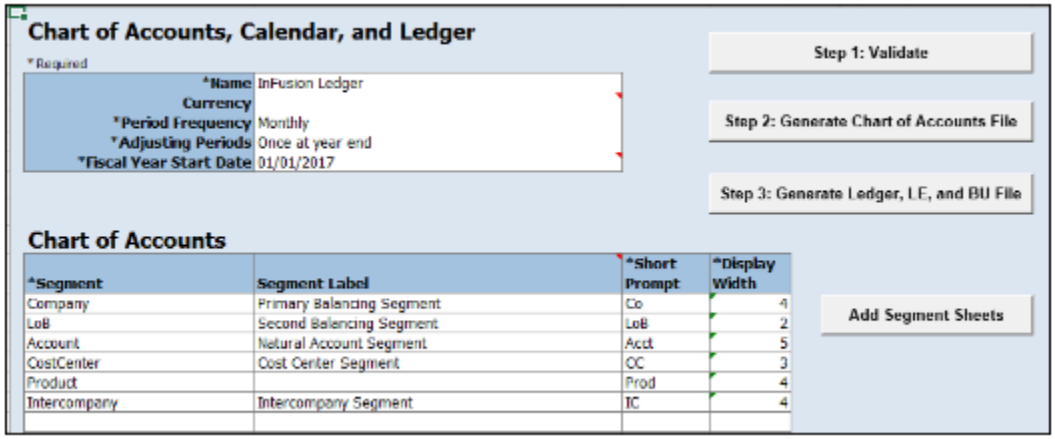
- Data preparation requirements
- Setup object concepts
- Best practices and recommendations
- Instructions on how to create additional hierarchies or hierarchy versions
- A completed workbook with sample data, which you can use to familiarize yourself with how to enter data, preview the sample report, and generate required upload files

Chart of Accounts, Calendar, and Ledger

Enter the data to create your chart of accounts, calendar, and ledger.

> **CAUTION:** Once you begin using your chart of accounts, calendar, and ledger, making changes to their fundamental attributes is neither recommended nor supported. This includes your chart of account segments, including the segment labels as well as other characteristics of those segments, and your calendar structure or pattern.

The following figure shows an example of the Chart of Accounts, Calendar and Ledger sheet with sample values.



An explanation of each field on the sheet follows.

- **Name**: Enter the name of your primary ledger.

  A primary ledger is created for each unique country that's entered in the Companies and Legal Entities sheet. A country code is appended to the name that you specify. For example, one legal entity is based in the United States and another in Canada. If you enter the ledger name of InFusion Ledger, two primary ledgers are automatically created, InFusion Ledger US and InFusion Ledger CA.

  All of the primary ledgers that are created use the same chart of accounts, account hierarchies, and accounting calendar. Legal entities and their primary balancing segment values are assigned to the primary ledger of their

respective countries. If the addresses provided for the legal entities on the Companies and Legal Entities sheet are all in the same country, then only one primary ledger is created.

- **Currency**: If you're not entering legal entities and only a single ledger should be created by the rapid implementation configuration, enter the ledger currency in which you want to maintain accounting for in that ledger. If you're entering legal entities, leave this field blank. The currency is automatically supplied based on the country.
- **Period Frequency**: Select from among the list of available frequencies for the ledger calendar.

  > **CAUTION:** For the accounting calendar created using the Rapid Implementation Enterprise Structure solution, the choices of patterns are limited to the period frequency and adjusting period options that are available for selection in the spreadsheet. It isn't possible to make alterations to the pattern or specified fiscal year start date once the calendar has already been created. The accounting periods of the calendar are automatically named using a preset format. If you want to change these period names, you have a limited window of time to make those changes. Use the Manage Accounting Calendars page in the application to make the changes before the accounting calendar is being used actively, such as when one of its accounting periods has been set to a status of Open.

- **Adjusting Periods**: Select the number of periods used to segregate closing, auditing, or other adjustments in General Ledger. The entries are tracked in the adjusting period and not in your monthly activity.
- **Fiscal Year Start Date**: Enter the start date of the accounting calendar. The date can't be changed after the submission of the configuration.

  > **CAUTION:** If you plan to run translations, enter a fiscal year start date for the entire accounting year that's before the first period for which you intend to run translations. You can't run translation in the first defined period of an accounting calendar. For example, if your fiscal year starts on January 1, and you want to start translations for the period of Mar-17, then you should select a fiscal year start date of January 1, 2016. Also when determining the fiscal year start date, you might want to consider whether you plan to load history.

- **Segment**: Enter the names for your segments. The value sets are created from the segments.
- **Segment Label**: Select segment labels to assign special functionality to segments.

  Segment labels specifying the segment's purpose, such as balancing, cost center and natural account, can only be assigned once to a chart of accounts segment. The **Primary Balancing Segment** and **Natural Account Segment** labels must be assigned, while the other segment labels are optional. Segments that are assigned these two particular labels cannot be assigned any other label. However, segments that are assigned the other remaining labels can also be assigned additional labels, provided they're not **Primary Balancing Segment** or **Natural Account Segment**.

  The **Intercompany Segment** label assignment is optional. If assigned, an Intercompany sheet is automatically added to the workbook when you select the **Add Segment Sheets** button. Use the sheet to enter your intercompany values and hierarchies. When you upload the chart of accounts file, the application creates a new value set for the Intercompany segment with the values that you entered. If you want to assign the Intercompany segment the same values as the Primary Balancing segment, copy all the parent and child values from the Companies and Legal Entities sheet to the Intercompany sheet.

  If you enable segment value security on the primary balancing value set, the security enforcement won't conflict with the Intercompany segment because the value sets for the two segments will be different. The same

holds true if you enable segment value security on the intercompany value set. Security enforcement won't conflict with the Primary Balancing segment.

If you plan to use related value sets and create a relationship between the segments that involves your primary balancing segment or intercompany segments, there won't be a conflict of values because the value sets are different.

> **Note:** If you want to assign the Intercompany segment the same value set as the Primary Balancing segment, you can change the value set assignment from the Manage Chart of Accounts Configurations page after you upload the chart of accounts configuration and before you upload the financial structures for the chart of accounts. If you decide to go with the same value set for both segments, you won't be able to change the value set association later on, once the ledger is assigned to the chart of accounts.

> **Note:** For the posting process to apply intercompany balancing, you must select the **Enable intercompany accounting** option on the Specify Ledger Options page.

- **Short Prompt**: Enter a short name for the segment, which is used on applications pages.
- **Display Width**: Enter the segment size. Select the size carefully and leave room for growth. For example, if you have 89 cost centers, enter 3 for the display length to allow for more than 100 cost centers in the future.
- **Add Segment Sheets**: Select this button to create sheets for additional segments. Sheets are provided only for the Company and Natural Accounts segments.

  From the new segment sheet, you can click the **Generate Additional Hierarchy** button to create more than one hierarchy for any chart of account segment. A worksheet is then automatically created and populated with the data already entered for that segment. Change this data as required for the new hierarchy. You can create additional hierarchies during initial setup, or after the initial setup is done.

> **CAUTION:** You can't change the chart of accounts, accounting calendar, or currency for your ledgers after the setup is created.

Business Units

Enter the name of your business units and related default legal entities.

The following figure shows an example of the Business Units sheet with sample values for the Name and Default Legal Entity Name fields.

Business Units

Name	Default Legal Entity Name
USA Business Unit1	VCC InFusion Cupertino Cherries
USA Business Unit2	VSCC InFusion San Carlos Chocolates
Canada Business Unit1	Infusion Core Canada Ltd.

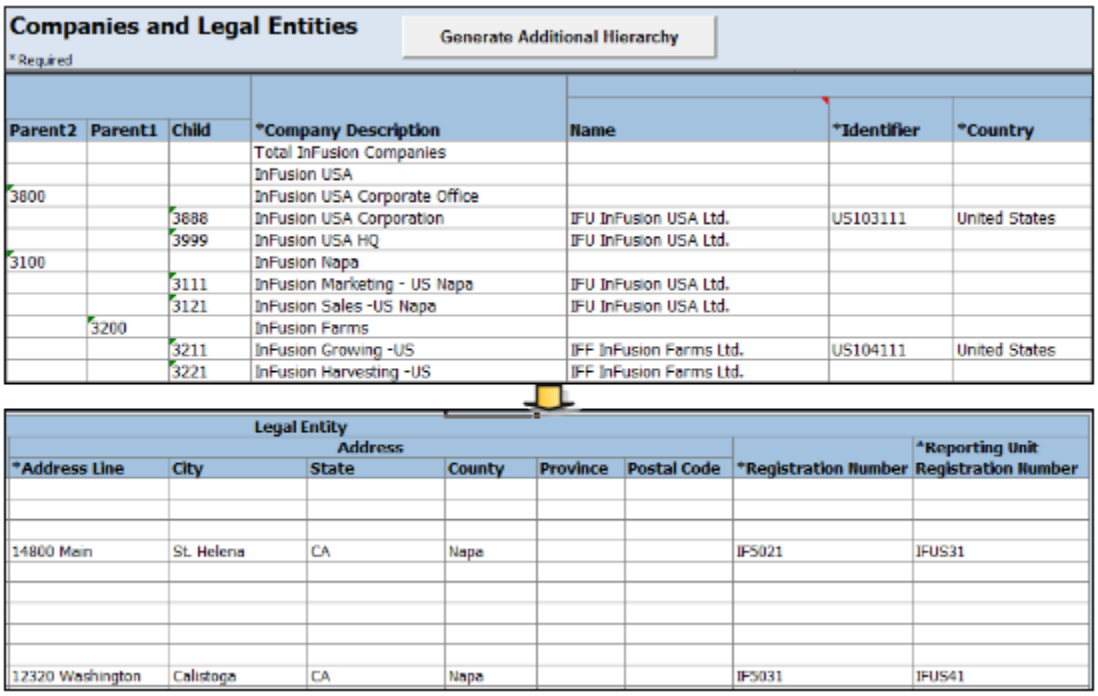
Business units are created with the names that you enter. You can enter more than one business unit per ledger. Based on the default legal entity specified for the business unit in the Business Units sheet, the business unit is assigned the primary ledger to which its default legal entity is assigned.

Companies and Legal Entities

Enter parent and child values for your Company segment, which is the segment that's assigned the Primary Balancing Segment label on the Chart of Accounts, Calendar, and Ledger sheet. You can create up to nine levels of parent values to roll up your companies to meet corporate and local reporting requirements.

Enter your legal entities for the child values with the address, registration number, and reporting unit registration number. The registration number identifies legal entities registered for your company and recognized by law for which you want to record and perform transactions. The reporting unit registration number identifies the lowest level component of a legal structure that requires registrations.

The following figure shows part of the Companies and Legal Entities sheet with sample values. The sheet includes columns for different levels of parent values, the child value, and company description. The Legal Entity columns include name, identifier, country, address information, and registration numbers.



Companies and Legal Entities

Generate Additional Hierarchy

*Required

Parent2	Parent1	Child	*Company Description	Name	*Identifier	*Country
			Total InFusion Companies			
			InFusion USA			
3800			InFusion USA Corporate Office			
		3888	InFusion USA Corporation	IFU InFusion USA Ltd.	US103111	United States
		3999	InFusion USA HQ	IFU InFusion USA Ltd.		
3100			InFusion Napa			
		3111	InFusion Marketing - US Napa	IFU InFusion USA Ltd.		
		3121	InFusion Sales -US Napa	IFU InFusion USA Ltd.		
	3200		InFusion Farms			
		3211	InFusion Growing -US	IFF InFusion Farms Ltd.	US104111	United States
		3221	InFusion Harvesting -US	IFF InFusion Farms Ltd.		

Legal Entity Address							
*Address Line	City	State	County	Province	Postal Code	*Registration Number	*Reporting Unit Registration Number
14800 Main	St. Helena	CA	Napa			IF5021	IFUS31
12320 Washington	Calistoga	CA	Napa			IF5031	IFUS41

To create additional hierarchies for the company segment for reporting or other purposes, click the **Generate Additional Hierarchy** button. A worksheet is automatically created and populated with the data already entered for that segment. Change this data as required for the new hierarchy. You can create additional hierarchies during initial setup, or after the initial setup is done.

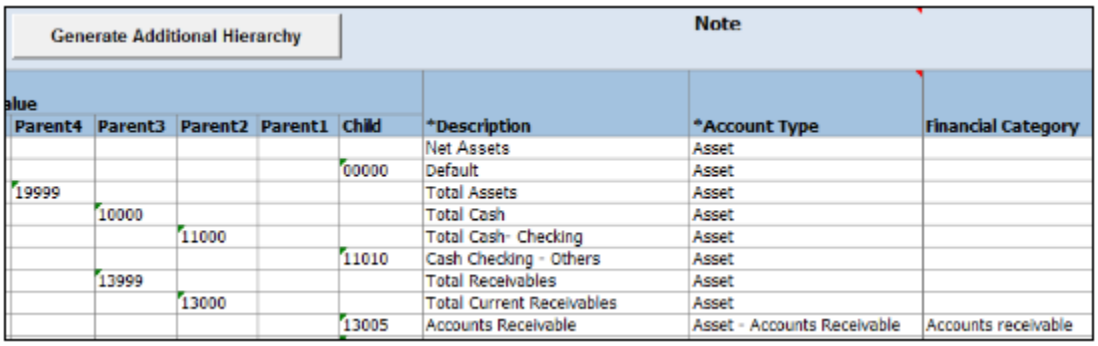
When a new hierarchy sheet is created, the name for that sheet is derived by adding a counter to the sheet name. For example, when you click **Generate Additional Hierarchy** on the Companies and Legal Entities sheet, the new sheet is named Companies and Legal Entities 1. When you click **Generate Additional Hierarchy** again, another sheet is generated with the name Companies and Legal Entities 2.

Note: Adding legal entity information isn't supported on a new hierarchy sheet for the Company segment.

Natural Accounts

Enter account hierarchies, account values, and specify account types.

The following figure shows part of the Natural Accounts sheet with sample parent and child values, descriptions, and account type.



Generate Additional Hierarchy | Note

alue Parent4	Parent3	Parent2	Parent1	Child	*Description	*Account Type	Financial Category
					Net Assets	Asset	
				00000	Default	Asset	
19999					Total Assets	Asset	
	10000				Total Cash	Asset	
		11000			Total Cash - Checking	Asset	
				11010	Cash Checking - Others	Asset	
	13999				Total Receivables	Asset	
		13000			Total Current Receivables	Asset	
				13005	Accounts Receivable	Asset - Accounts Receivable	Accounts receivable

- **Parent**: Enter parent account values to define hierarchies. Hierarchies are used for chart of accounts mappings, revaluations, data access sets, cross-validation rules, and segment value security rules. The balances cube and account hierarchies are also used for financial reporting, Smart View queries, and allocations.
- **Child**: Enter child account values to define the postable accounts.
- **Description**: Enter descriptions for the segment values.
- **Account Type**: You must assign an account type to each account value. Account types are used in year-end close processes and to correctly categorize account balances for reporting. Select from among general account types and expanded account types. The general account types are: **Asset**, **Liability**, **Owner's Equity**, **Revenue**, **Expense**. Expanded account types provide specialized functionality and are used to:
    - Identify the intended usage of your natural account values to facilitate automation and enable completion of other required setup objects. For example, assign the **Asset** - **Intercompany Receivable** and **Liability** - **Intercompany Payable** expanded account types. The Rapid Implementation process then automatically creates a chart of accounts level intercompany balancing rule, which is a required setup for the application to perform intercompany balancing.
    - Automatically generate fully defined initial Financial Reporting reports and Account Groups based on your enterprise structure.

  Examples of expanded account types include:

    - **Asset** - **Accounts Receivable**: For Receivables receipt methods
    - **Liability** - **Accounts Payable**: For Payables common options
    - **Owner's Equity** - **Retained Earnings**: For General Ledger ledger options
    - **Revenue** - **Top Revenues Parent Account**: For sample reports and account groups
    - **Expense** - **Top Operating Expenses Parent Account**: For sample reports and account groups

  You must assign the **Revenue** - **Top Revenues Parent Account** and **Expense** - **Top Operating Expenses Account** account types to the parent accounts that are your highest level and comprehensive revenue and operating expenses accounts. You can optionally assign the account type of **Expense** - **Top Cost of Sales Parent Account**, if it's applicable for your scenario.

  The **Generate Financial Reports and Account Groups** process, which is automatically submitted when the accounting configuration is created in the application, generates a set of Financial Reporting reports and

account groups according to the accounting configuration defined in the workbook. The top parent accounts are used as the basis for deriving the accounts referenced in the reports and in the Account Groups.

The immediate descendants of the top parent accounts are used to define the rows on the reports. Depending on whether both the top operating expense and top cost of sales accounts are tagged, different variations of the income statements are generated. If the optional top cost of sales account is provided, the Financial Reporting reports that are income statements also include a gross margin section.

> **CAUTION:** Assign account types carefully. If you assign an incorrect account type to a natural account segment value, accounting entries are recorded incorrectly and financial statements are inaccurate. Misclassified accounts are also potentially handled incorrectly at year end, with actual balances either getting zeroed out to retained earnings, or accumulating into the next year.

- **Financial Category**: Select a value to identify groups of accounts for reporting with Oracle Transactional Business Intelligence. You can add financial categories to parent values. Accounts that are tagged with expanded account types are automatically assigned a financial category. You can override the default category or leave it out.

  > **Note:** The list of accepted values is defined in the FINANCIAL_CATEGORY lookup_type.

- **Generate Additional Hierarchy**: To create additional hierarchies for the natural account segment for reporting or for other purposes, click the **Generate Additional Hierarchy** button. A worksheet is automatically created and populated with the data already entered for that segment. Change this data as required for the new hierarchy. You can create additional hierarchies during initial setup or after the initial setup is done.

Financial Sequences

Enable document or journal sequences to assign unique numbers to transactions to meet legal requirements.

The following figure shows the Financial Sequences sheet with sample values for the Restart and Initial Value columns.

Sequences

Transactions	*Restart	*Initial Value
Payables Invoices	Annually	1
Payments	Annually	1
Receivables Invoices	Annually	1
Receivables Credit Memos	Annually	1
Receivables Adjustment Activities	Monthly	1
Subledger Journals	Never	100
General Ledger Journals	Never	100

Document sequences are created for these transactions: Payables invoices, Payments, Receivables invoices, Receivables credit memos, Receivables adjustment activities. Reporting and accounting journal sequences are created for Subledger journals and General Ledger journals.

For each transaction, you can provide values for the following fields:

- **Restart**: Set when to restart the numbering: Annually, Monthly, Never.
- **Initial Value**: Specify the beginning number in the sequence.

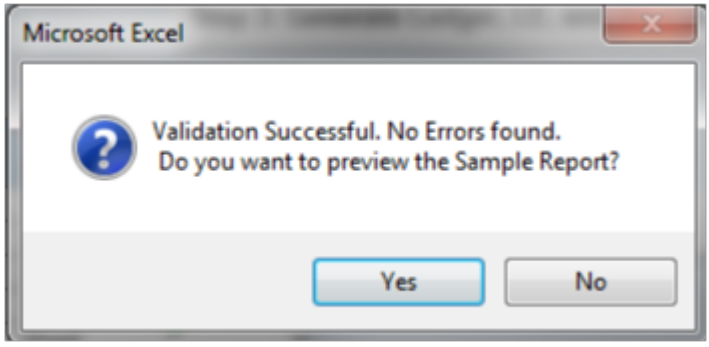
How Worksheets Are Processed

After you complete the worksheets, proceed with validation, sample report preview, and file upload.

1. On the Chart of Accounts, Calendar, and Ledger sheet, click the **Step 1**: **Validate** button.

   The validation checks the worksheets for missing or inappropriate setups. Errors are marked as actionable items in a validation report sheet that's dynamically generated. You can review the anomalies and make the corrections as indicated. The **Field** column on the validation report notes the issue. Click the text link to navigate to the appropriate field in the sheet that must be updated. When the validation is successful, a message appears with the option of previewing a sample of the reports that are automatically generated as part of the enterprise configuration.

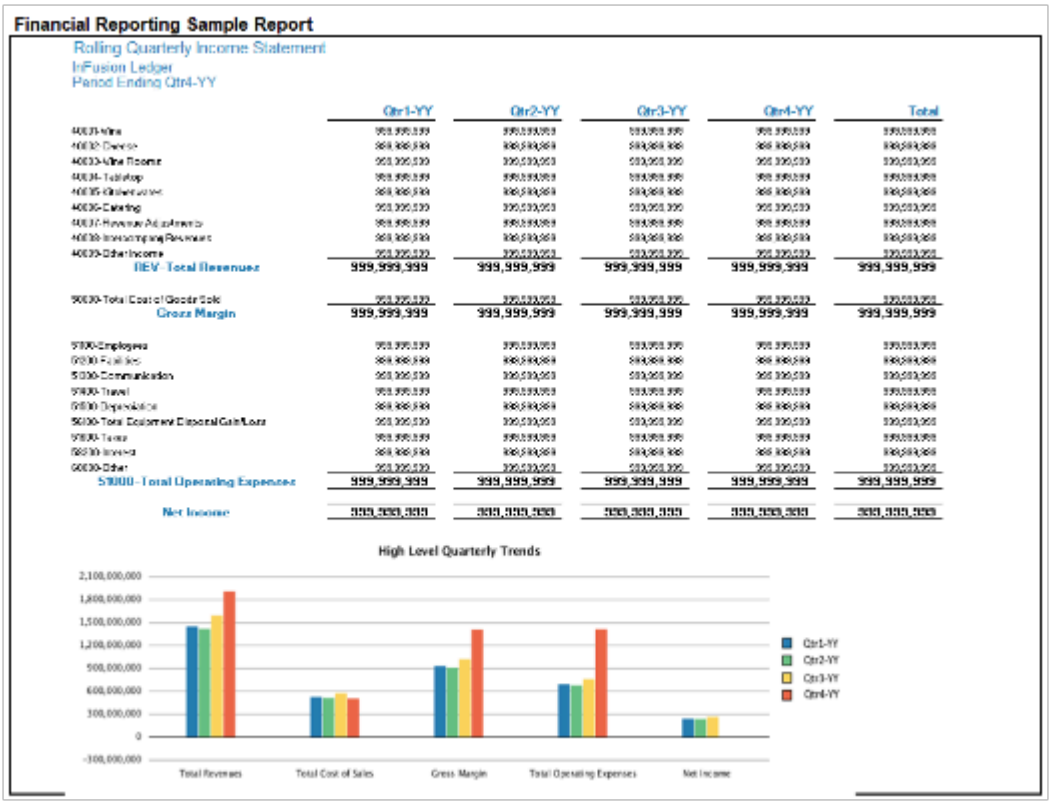
   The following figure shows the message that appears after a successful validation.



   If you select to preview the sample report, a new sheet is automatically created called Preview Report. The preview incorporates elements of the setup that you provided. The rows on the report are derived based on the

top parent revenue and expense account values that you tagged on the Natural Accounts sheet. The preview also reflects the reporting hierarchy for your natural accounts.

The following figure shows an example of the sample Financial Reporting report.



You can use the preview to validate whether the hierarchy setup aligns to your reporting needs. If the natural account hierarchy requires adjustments, this is your chance to make those corrections before actually creating the account hierarchies in the application. You can modify your enterprise structure setup, validate the spreadsheet, and preview the revised sample reports for as many times as you need. The account hierarchies are created when you finally submit the accounting configuration in the rapid implementation spreadsheet.

2. Click **Step 2**: **Generate Chart of Accounts File**. The process generates a data file called **ChartOfAccounts.xml** with the entered chart of accounts and hierarchies setup data. Save the file to a network or local drive.
3. Click **Step 3**: **Generate Ledger**, **LE**, **and BU File**. The process generates a data file called **FinancialsCommonEntities.xml** with the entered ledger, legal entities, and business unit setup data. Save the file to a network or local drive.
4. From your implementation project, go to the **Upload Chart of Accounts** task. The Upload Enterprise Structures and Hierarchies process is launched.
5. Accept the default selection of the **Upload Enterprise Structure** option.
6. Click **Browse** and select the first file that you saved called **ChartOfAccounts.xml**.
7. Click **Submit**.
8. Verify that the process completed without errors or warnings.
9. From your implementation project, go to the **Upload Ledger**, **Legal Entities**, **and Business Units** task. The **Upload Enterprise Structures and Hierarchies** process is launched.
10. Accept the default selection of the **Upload Enterprise Structure** option.

11. Click **Browse** and select the second file that you saved called **FinancialsCommonEntities.xml**.
12. Click **Submit**.
13. Verify that the process completed without errors or warnings.

An individual set of the following Financial Reporting reports is generated for each ledger that's defined within the rapid implementation accounting configuration. If multiple primary ledgers are created as part of your configuration, a set of Financial Reporting reports is generated for each ledger.

- Income Statement
- Consolidated Income Statement
- Rolling Quarterly Income Statement
- Rolling Monthly Income Statement
- Trial Balances by Ledger Currency
- Trial Balances by Entered Currency

The process also generates three account groups. These include two for the infolets, Revenues and Expenses, and one for the Close Monitor called Close Monitor Summary Income Statement. A set of these three account groups is generated for the balances cube, to be shared among all the ledgers that are part of that balances cube.

Additional Hierarchies After Initial Setup

To create additional hierarchies and hierarchy versions, or to update existing hierarchy versions after the initial setup:

1. Click the **Generate Additional Hierarchy** button on the applicable segment sheet. A new worksheet is automatically created and populated with the data already entered for that segment. Change the data as required.
2. Click the **Generate File for This Hierarchy Only** button. This generates a .zip file for the particular hierarchy.
3. From your implementation project, go to the **Upload Chart of Accounts** task. The **Upload Enterprise Structures and Hierarchies** process is launched.
4. Select the **Upload Hierarchy** option.
5. Select from among the following options and provide values for the required parameters:
    a. Create hierarchy: Select to create another account hierarchy. Specify the value set, tree code, and start date.
    b. Create version: Select to render a new version of an existing account hierarchy. Specify a value set, tree code, tree version, and start date.
    c. Update existing version: Select to edit an existing version of an account hierarchy. Specify a value set, tree code, and tree version.
6. Click **Choose File** and select the .zip file that you saved earlier.
7. Click **Submit**.

Related Topics

- Overview of Trees
- How Financial Reporting Reports and Account Groups Are Generated
- Manage Setup Using Implementation Projects

Overview of Cross-Validation Rules in General Ledger

You can use cross-validation rules to determine the valid account combinations that can be dynamically created as users enter transactions or journal entries.

Once enabled, a cross-validation rule determines whether a selected value for a particular segment of an account combination can be combined with specific values in other segments to form a new account combination.

For example, your organization has determined that the company Operations can't use the Marketing cost center. You can define a cross-validation rule such that, if the company is Operations, then validate that the cost center isn't Marketing. New account combinations have to satisfy all of the cross-validation rules enabled for the chart of accounts before they can be created.

Entry and Maintenance

This table describes the different methods that you can use to enter and maintain cross-validation rules.

Method	Navigation	What You Can Do
Manage Cross-Validations page, Rules tab	In the Setup and Maintenance work area, use the **Manage Cross-Validation Rules** task in the Financial Reporting Structures functional area. **Note:** As an alternative navigation, select the **Manage Cross-Validation Rules** action on the Manage Chart of Accounts Configuration page.	• Create • Edit • View • Upload to the interface table • Download from the interface table • Import from the interface table into the application • Download from the application • Submit the **Manage Account Combination Validation Rules** process
Cross-Validation Rules Import file-based data import (FBDI)	Access the FBDI template from either of these locations: 1. In the Oracle Help Center (https://docs.oracle.com), open the Oracle Fusion Cloud Financials File-Based Data Import (FBDI) for Financials guide. 2. In the Setup and Maintenance work area, use the **Manage Cross-Validation Rules** task in the Financial Reporting Structures work area.	Create and edit large volumes of cross-validation rules
Create Cross-Validation Rules desktop-integrated spreadsheet	In the Setup and Maintenance work area, use the **Create Cross Validation Rules in Spreadsheet** task in the General Ledger functional area.	Create a large volume of cross-validation rules.

To edit error messages for cross-validation rules, use this task in the Setup and Maintenance work area:

- Offering: Financials

- Functional Area: Financial Reporting Structures
- Task: Manage Messages for General Ledger

Tip: When you export or import cross-validation rules to a new instance using an export or import project in the Functional Setup Manager, you must add the **Manage Messages for General Ledger** task before the **Manage Cross-Validation Rules** task. You must export or import the messages before exporting or importing the cross-validation rules.

Existing Account Combinations

If existing account combinations violate newly enabled cross-validation rules, those account combinations continue to be valid. Before you disable existing account combinations that violate your rules and that you no longer use, move the balances in those accounts to the correct accounts. Then disable the account combinations to prevent further posting. Best practice is to define and enable cross-validation rules before account combinations are created, transactions or journal entries are imported or entered, and balances are loaded.

Related Topics

- Cross-Validation Rules
- Considerations for Cross-Validation Rules
- Create Cross-Validation Rules in a Spreadsheet
- How Cross-Validation Rule Violations Are Managed
- How do I update existing setup data?

Cross-Validation Rules Spreadsheet

The rapid implementation solution provides a template for defining cross-validation rules in a spreadsheet.

Cross-validation rules determine whether a selected value for a particular segment of an account combination can be combined with specific values in the other segments to form a new account combination.

In the Setup and Maintenance work area, use the following:

- Offering: Financials
- Functional Area: General Ledger
- Task: Create Cross Validation Rules in Spreadsheet

Note: The spreadsheet can only create cross-validation rules. To update existing cross-validation rules, use the **Manage Cross-Validation Rules** task in the Setup and Maintenance work area.

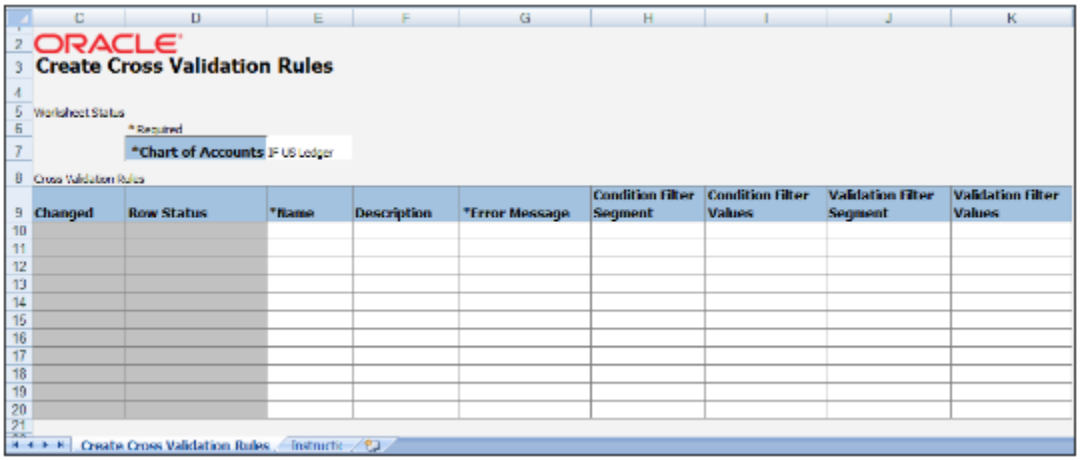
Spreadsheet Overview

The cross-validation rules spreadsheet includes two sheets. One sheet has instructions and the other sheet provides the template for creating the cross-validation rules. The Instructions sheet includes:

- An overview

- An explanation of the template
- Steps to fill in the template
- An example

The following figure shows the Create Cross-Validation Rules sheet.



The following table describes each field and column on the sheet.

Field or Column	Description
Worksheet Status	The upload results for the worksheet. The application updates this field when you submit the spreadsheet.
Chart of Accounts	The chart of accounts for which the cross-validation rules are defined.
Changed	The indicator that the row has been updated. The application updates this field.
Row Status	The upload results for the row. The application updates this field when you submit the spreadsheet.
Name	The name that uniquely identifies the cross-validation rules in a deployment.
Description	The purpose for the cross-validation rule.
Error Message	The explanation to users for why the attempted combination violates the cross-validation rule.
Condition Filter Segment	The segments of the chart of accounts that constitute the condition filter.
Condition Filter Values	The values of the condition filter segment that determine whether the cross-validation rule is evaluated.
Validation Filter Segment	The segments of the chart of accounts that constitute the validation filter.
Validation Filter Values	The values of the validation filter segment used to enforce a new account combination.

Field or Column	Description

Note: Cross-validation rules created from the spreadsheet are automatically enabled and don't have a start or end date.

Steps to Use the Template

To use the spreadsheet template:

1. Select the chart of accounts.
2. Enter a suitable name, description, and error message in the respective columns.
3. Select the condition filter segment. To add more than one segment to the condition filter, use the next row. Repeat the rule name and select the condition filter segment.
4. Provide the segment values that constitute the condition filter in the **Condition Filter Values** column.
    - To select multiple detail values, enter the detail values separated by commas. For example: **5501,5502,5503**.
    - To select a range, enter the detail values separated by hyphens. You can enter multiple ranges using the comma as the range separator. For example: **3001-3030,3045-3200**.
    - To select all detail values that are descendants of a parent, enter the parent value. You can enter multiple parent values using commas as the separator. For example: **1000,2000**.
    - You could enter all of the previously listed values in the same cell. For example: **1000,2000,3001-3030,3045-3200,5501,5502,5503**.
    - To specify that a detail value should not be selected, prefix the value with the less than and greater than symbols <>. These symbols represent the Does Not Equal operator. For example, <>5501 means the rule applies when the segment value isn't equal to 5501.
        - This operator can't be used for parent values or ranges.
        - This operator can't be used more than once for the same rule and segment.
5. Select the validation filter segment. To add more than one segment to the validation filter, use the next row. Repeat the rule name and select the validation filter segment.
6. Provide the segment values that constitute the validation filter in the **Validation Filter Values** column in the same way as specified for the condition filter.
7. Review the data that you entered and click **Submit** to publish the cross-validation rules.
8. Review the upload results in the **Worksheet Status** and **Row Status** fields.

Related Topics

- Cross-Validation Rules
- Considerations for Cross-Validation Rules
- Create Cross-Validation Rules in a Spreadsheet
- How do I update existing setup data?

Overview of Cash Management Rapid Implementation

Use Microsoft Excel templates to rapidly implement the following setup objects:

- Banks
- Bank Branches
- Bank Accounts

Functional Setup Manager Tasks

The following are the Functional Setup Manager tasks that are required to be performed to rapidly create the setup objects data. To access these tasks, create an implementation project that includes the Define Financials Configuration for Rapid Implementation task list:

- Create Banks, Branches, and Accounts in Spreadsheet: Downloads the rapid implementation excel spreadsheet template. Enter the bank, branch, and bank account data in this spreadsheet, and generate the data file to be loaded.
- Upload Banks, Branches, and Accounts: Launches the Upload Banks, Branches, and Accounts process with the data file to be uploaded as the parameter. You must upload the data file generated from the previous task.

Preparing Data

Prepare your bank, branch, and account information to enter into the spreadsheet template.

- Bank information requires the country, name, and number.
- Branch information requires name, number, BIC code, and alternate name.
- Account information requires name, number, currency, legal entity, type, and IBAN.

After you finish preparing the data in the spreadsheet, click the Generate Banks, Branches, and Accounts File button. Save the generated XML file.

Loading Data

Use the following steps to load your data.

- In the Setup and Maintenance work area, create an implementation project that includes the Define Financials Configuration for Rapid Implementation task list. From your implementation project, go to the Upload Banks, Branches, and Accounts task. This task launches the Upload Banks, Branches, and Accounts process.
- Select the XML file you have saved earlier and submit the process.
- Verify in the process monitor that the process completed successfully.
- Review the banks, branches, and accounts created.

Best Practices

The following are recommended best practices:

- Determine the Legal Entity for each bank account. The Legal Entity must be associated to a primary ledger.
- Determine the use for each bank account: Payable, Receivable, or both.
- Determine the Cash and Cash Clearing account for each bank account. Enter the entire account combination based on your chart of accounts, for example 01-000-1110-0000-000.

Related Topics

- How You Process Electronic Bank Statements

Tax Configuration Workbook

Use the Tax Configuration Workbook to upload all common tax setups. For example, create standard state, county, and city sales tax rates within the US using this workbook.

Tax Configuration Workbook Worksheets

The Tax Configuration Workbook is a Microsoft Excel spreadsheet template with six common tax setup worksheets:

Worksheet	Predefined Data Content	Setup Options
Manage Tax Regimes	Yes	Option 1: Use the tax regimes that are already included for 28 countries. You can modify or delete any of the predefined tax regimes where needed. Option 2: Use tax partner content for the Tax Configuration Workbook.
Manage Taxes	Yes	Option 1: Use the taxes that are already included for 28 countries. You can modify or delete any of the predefined taxes where needed. Option 2: Use tax partner content for the Tax Configuration Workbook.
Manage Tax Zones	No	Prepare the tax zones with the appropriate corresponding geographies.
Manage Rates	No	Option 1: Prepare the tax rates. Option 2: Use tax partner content for the Tax Configuration Workbook.

Worksheet	Predefined Data Content	Setup Options
Manage Tax Thresholds	No	Option 1: Prepare the tax thresholds or maximum taxes. Option 2: Use tax partner content for the Tax Configuration Workbook.
Manage Tax Recovery Rates	No	Option 1: Prepare the tax recovery rates. Option 2: Use tax partner content for the Tax Configuration Workbook.

Related Topics

- Example of Creating Tax Setup Using the Tax Configuration Workbook
- Example of Creating Tax Setup Using Tax Partner Content in the Tax Configuration Workbook

Example of Creating Tax Setup Using the Tax Configuration Workbook

This example shows how you can create standard sales tax rates within the US using the Tax Configuration Workbook. You can create sales tax rates at state, county, and city levels using this method.

Here's a summary of key decisions you make in this scenario:

Decision to Consider	In This Example
What tax setup are you creating?	Tax Rates
Do you have exception rules for calculating US sales tax on transactions?	No
Do you use tax partner content?	No

Creating Tax Setup

Follow these steps to create tax rates in the Tax Configuration Workbook:

1. Navigate to the Manage Tax Regimes page.
2. Click the **Rapid Setup Spreadsheets** button and select **Download Tax Configuration Workbook**.
3. Save the Tax Configuration Workbook in your local directory.
4. Review the details on the Instructions sheet of the workbook.
5. For the Manage Tax Regimes and Manage Taxes worksheets, use the predefined content for the US sales tax. You can modify or delete the predefined content where needed.

6. Use the instructions and the column help text to populate the required setups in the Manage Rates worksheet.
7. After completing the Tax Rates worksheet, go to Instructions sheet again.
8. Click **Generate CSV File**. It performs theses actions:
    - Saves the entire Tax Configuration Workbook data in a comma separated values (CSV) file.
    - Saves the CSV file into a single compressed file attachment.
9. Save the compressed file attachment in your local directory.
10. Click the **Rapid Setup Spreadsheets** button and select **Upload Tax Configuration Workbook.**
11. Select the compressed file that you saved earlier.
12. Click **Open** and then click **Upload**.
13. Note the process ID and click the Monitor Upload and Download Processes tab.
14. Click **Refresh** and ensure that the process ID completes with a Succeeded status.
    - If the status of the upload process is Succeeded, you can view your setups using the search criteria on the page.
    - If the status of the upload process isn't Succeeded, your upload has failed. Check the details in the corresponding error log, correct any file errors, and reupload the file.

Related Topics

- Example of Creating Tax Setup Using Tax Partner Content in the Tax Configuration Workbook

Guidelines for Uploading Customer Data Using a Simplified Spreadsheet

Use the Upload Customers from Spreadsheet process to upload customer data using the simplified Customer Import FBDI (File-Based Data Import) template.

The single upload process performs all the operations of generating a batch, transferring the customer data in the spreadsheet template to the interface tables, and importing the data from the interface tables into Oracle Applications.

Download the simplified Customer Import FBDI template and prepare your customer data. The template contains an instruction sheet and sample data to help guide you through the process of entering your customer information: Customers, Contacts, Reference Accounts, Customer Bank Accounts.

> **Note:** You can also use the Customer Import process to download a Customer Import FBDI template, available from the FBDI Customer Data Model, to prepare and upload customer data into Receivables and the Trading Community Model registry.

Set Up Related Customer Information

Set up the business objects you need in advance of the customer data upload.

This can include:

- Account address sets: Set up the reference data sets you need for your customer account sites.
- Customer profile classes: Set up one or more profile classes for your customer records.

- Reference accounts: Set up general ledger accounts that you intend to use as reference accounts for customers.
- Customer bank accounts: Set up banks and bank account information.
- Tax information: Set up tax registration numbers and tax rate codes using Oracle Tax.
- Descriptive flexfields.

Enter Data in the Spreadsheet Columns

Enter data in the designated columns in each of the four worksheets: Customers, Contacts, Reference Accounts, Customer Bank Accounts.

These rules apply to entering data in columns:

- Column labels with an asterisk (*) denote required columns.
- Use the **Show Extensible Attributes** and **Hide Extensible Attributes** buttons to show or hide additional columns.
- Don't move or delete existing columns, and don't insert new columns.
- Enter data in the correct format. In most cases, the columns will format the data that you enter according to the requirements of the upload.
- To remove existing values from specific fields in an existing customer profile, enter the exclamation point character (!) in the corresponding column.
- Each customer must have a unique combination of these values:
  - Customer number.
  - Customer account number.
  - Customer site number.
- Each customer contact must have a unique person number.

Examples of Validations in Customer Spreadsheet Upload Data

During upload processing, the Upload Customers from Spreadsheet process checks for unique values in certain columns of the Customers and Contacts worksheets. If the values are unique, the record is created. If the values aren't unique, the record fails with an upload error.

The columns with this validation are:

- Customers worksheet:
  - Customer Number
  - Account Number
  - Site Number
- Contacts worksheet:
  - Person Number

The following sections provide examples of the validation process. The assumption in these examples is that all records have the same Source System value.

Customers Worksheet: Customer Number Validation

The Customer Number validation looks for a unique combination of values across the Customer Number, Customer Source Reference, and Customer Name columns.

The records in the following table fail the uniqueness validation on the customer number, because, for the same customer name, there are two different customer numbers and customer source references.

Customer Number	Customer Source Reference	Customer Name
VCORP 256113	VCORP 256113	Vision Corporation
VCORP 256114	VCORP 256114	Vision Corporation

The records in the following table also fail the uniqueness validation on the customer number, because, for the same combination of customer number and customer source reference, there are two different customer names.

Customer Number	Customer Source Reference	Customer Name
VCORP 256113	VCORP 256113	Vision Corporation
VCORP 256113	VCORP 256113	Vision ABC Corporation

The records in the following table also fail the uniqueness validation on the customer number, because, for the same customer number, there are two different customer source references.

Customer Number	Customer Source Reference	Customer Name
VCORP 256113	VCORP 256113	Vision Corporation
VCORP 256113	VCORP 256114	Vision Corporation

In like manner, the Account Number validation looks for a unique combination of values across the Account Number, Account Source Reference, and Account Description columns. The Site Number validation looks for a unique combination of values across the Site Number, Site Source Reference, and Site Name columns.

Contacts Worksheet: Person Number Validation

The Person Number validation looks for a unique combination of values across the Person Number, Person Source Reference, and First Name and Last Name columns.

The records in the following table fail the uniqueness validation on the person number, because, for the same combination of person number and person source reference, there are two different first name and last name combinations.

Person Number	Person Source Reference	First Name	Last Name
1000228801	1000228801	Rodney	Jones
1000228801	1000228801	John	Jones

The records in the following table also fail the uniqueness validation on person number, because, for the same person number, there are two different person source references.

Person Number	Person Source Reference	First Name	Last Name
1000228801	1000228801	Rodney	Jones
1000228801	1000228802	Rodney	Jones

The records in the following table pass the uniqueness validation. The validation process allows a combination of two different person numbers and person source references with the same first name and last name combination. This is because two different people may have the same name.

Person Number	Person Source Reference	First Name	Last Name
1000228801	1000228801	Rodney	Jones
1000228802	1000228802	Rodney	Jones

Budget Uploads to General Ledger

Overview of Budget Uploads

In Oracle General Ledger, you can load budget data to perform variance reporting.

If you use a third-party budgeting application or don't use a budgeting application, there are two ways to load budgets into the GL Balances Cube.

- **Importing Budget Data from a Flat File**: Export budget data from your budgeting application to a comma separated values .csv file. Use the Import General Ledger Budget Balances file-based data import (FBDI)

to prepare and generate flat files in a .csv format. You can use Oracle ADF Desktop Integrator correction worksheets to correct validation errors, delete rows with errors, and resubmit the corrected error rows.

> **Note:** For more information about FBDI, see the Oracle Fusion Cloud Financials File-Based Data Import (FBDI) for Financials guide.

- **Importing Budget Data from a Spreadsheet**: You can access the budget load spreadsheet from the General Accounting Dashboard. Enter, load, and correct budget data in the ADF Desktop Integrator spreadsheet tool. Use this tool to prepare and load budget data for multiple ledgers and periods with a common chart of accounts instance. The list of values and the web picker help you select valid values. This simplified data entry reduces errors and alerts you to errors as you enter the data in the spreadsheet. Error correction is done in the same spreadsheet.

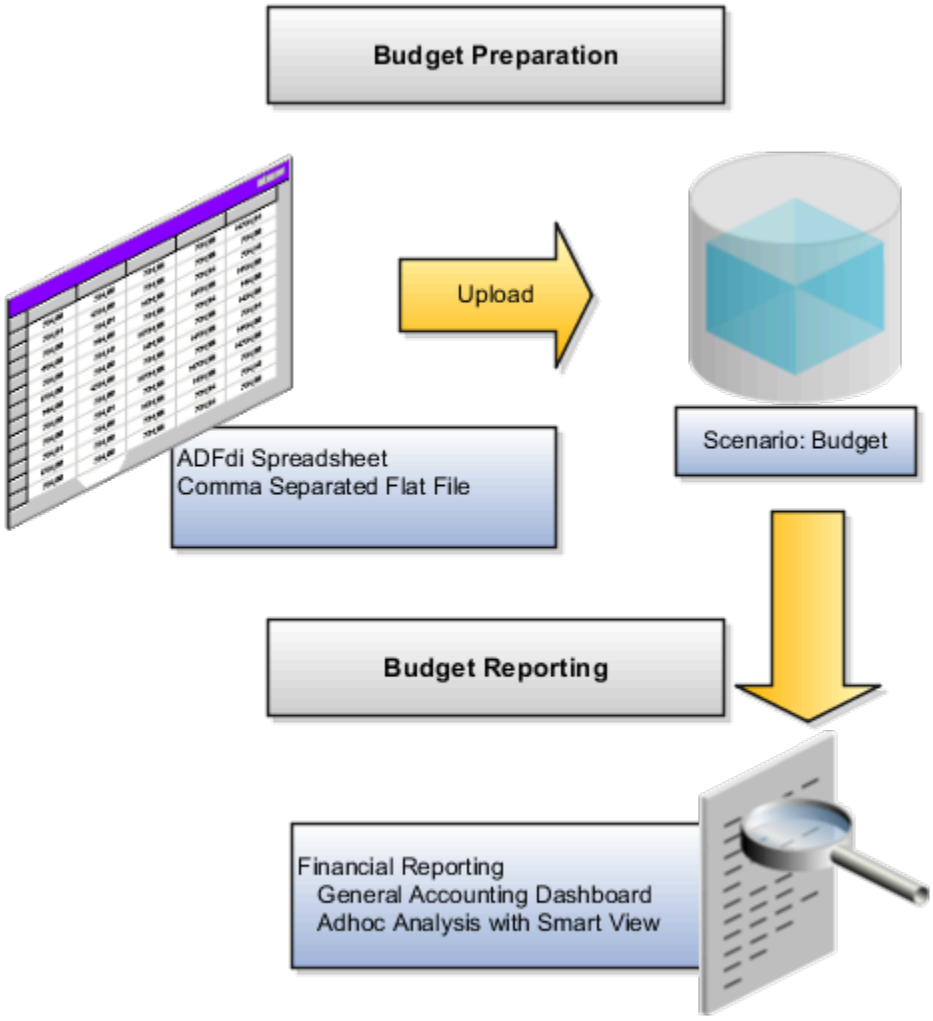
Here are some points to consider when preparing your budget data.

- You can maintain budget amounts only for detail accounts. However, if you're also using budgetary control, you can configure your setup to maintain budget amounts for summary accounts.

> **Note:** For more information about budgetary control setup, refer to the Budgetary Control chapter, Enterprise Options section in the Oracle Fusion Cloud Financials Using Financials for the Public Sector guide.

- If you already uploaded your budget and you perform another upload using the same criteria, the upload process overwrites the existing amounts with the amounts from the new upload.

The following figure shows the process flow for budget upload. Prepare your budget data, upload it using a spreadsheet or flat file, and report on the budget data.



CAUTION: When the GL Balances Cube is rebuilt, the process retains the budget balances as well as the actual balances. Only the budget balances loaded using the spreadsheet or flat file through the GL Budget Balances interface table are retained. Create reports in **Smart View** or **Financial Reporting** to verify that the budget data was loaded correctly.

Related Topics

- Import Budget Data from a Spreadsheet
- How General Ledger Budget Balance Import Data Is Processed
- Overview of Enterprise Options

Import Budget Data from a Spreadsheet

You can use the Create Budgets spreadsheet to enter, load, and correct budget data. To open the spreadsheet, navigate to the General Accounting Dashboard and select the Create Budgets in Spreadsheet task.

Budget Import

The spreadsheet uses the Oracle ADF desktop integration add-in for Excel, which is the same add-in used by the Create Journals spreadsheet. The spreadsheet uses an interface table called GL_BUDGET_INTERFACE and requires the Budget Entry role. The budget import uses the Accounting Scenario value set for the budget being loaded. The Run Name is used as an identifier for the imported data set.

The spreadsheet budget import:

- Supports multiple ledgers but a single chart of accounts instance
- Allows multiple calendars and periods
- Supports entered currencies in addition to the ledger currency
- Contains user-friendly lists of values
- Performs most validations on the worksheet
- Secures values by data access sets

Note: The spreadsheet includes a **Row Status** column that shows if the rows upload successfully or with errors. Use the spreadsheet where the data was entered to enter the corrections.

How General Ledger Budget Balance Import Data Is Processed

Use the Import General Ledger Budget Balances file-based data import (FBDI) to load budget data from external sources for upload to the GL balances cube. You can download a budget spreadsheet template to use to prepare your budget data.

The template contains an instruction sheet to help guide you through the process of entering your budget information.

To access the template, complete the following steps:

1. Navigate to the Oracle Fusion Cloud Financials File-Based Data Import (FBDI) for Financials guide.
2. In the table of contents, click **General Ledger**.
3. Click **Import General Ledger Budget Balances**.
4. In the File Links section, click the Excel template.

Follow these guidelines when preparing your data in the worksheet:

- Enter the required information for each column. Refer to the tool tips on each column header for detailed instructions.
- Don't change the order of the columns in the template.
- You can hide or skip the columns you don't use, but don't delete them.

Settings That Affect the General Ledger Budget Balances Import Process

The Import General Ledger Budget Balances template contains an instructions tab and a tab that represents the table where the data is loaded.

The Instructions and CSV Generation tab contains information about:

- Preparing the budget data.
- Understanding the format of the template.
- Entering budget data.
- Loading the data into the interface table and the GL balances cube.

The GL_BUDGET_INTERFACE tab is where you enter information about the budget data that you adding, such as the ledger, budget name, periods, segment values, and amounts.

How General Ledger Budget Balance Import Data Is Processed

To load the data into the interface table:

1. Click the **Generate CSV File** button on the instructions tab to create a CSV file in a .zip file format.
2. Save the .zip file locally.
3. Navigate to the Scheduled Processes work area.
4. Select the **Load Interface File for Import** process.
5. For the **Import Process** parameter, select **Validate and Upload Budgets**.
6. For the **Data File** parameter, select the file that you saved in step 2.

To load the data from the interface table to the balances cube:

1. Navigate to the Scheduled Processes work area.
2. Select the **Validate and Upload Budgets** process.
3. Enter values for the **Run Name** parameter.
4. If the process ends in error or warning:
    a. Review the log and output files for details about the rows that caused the failure.
    b. Navigate to the General Accounting Dashboard work area.
    c. Select the **Correct Budget Import Errors** task to download the budget corrections worksheet.
    d. Correct the entries in the worksheet and resubmit the Validate and Upload Budgets process.

Related Topics

- Overview of External Data Integration Services for Importing Data
- Import Budget Data from a Flat File
- Load Budgets
- External Data Integration Services for Importing Data

Import Budget Data from a Flat File

Use the upload budgets processes to integrate budget information from other budgeting applications such as Oracle Hyperion Planning.

Use the Import General Ledger Budget Balances file-based data import (FBDI) to load budget data from external sources for upload to the GL balances cube.

You can load your budget amounts to the General Ledger balances cube by populating the GL_BUDGET_INTERFACE table and running the Validate and Upload Budgets process. You can load budgets for multiple periods and for multiple ledgers with the same chart of accounts in a single load process.

> **Note:** Budget data isn't loaded to the GL_BALANCES table and only loaded to the balances cube for variance reporting purposes.

Assigning Values for Columns in the GL_BUDGET_INTERFACE Table

For budget import to be successful, you must enter values in the columns of the interface table that require values.

The following table describes the columns that require values.

Name	Value
RUN_NAME	Enter a name to identify the budget data set being imported.
STATUS	Enter the value NEW to indicate that you're loading new budget data.
LEDGER_ID	Enter the appropriate ledger ID value for the budget amount. You can view the ledger ID for your ledgers on the Manage Primary Ledgers page. The ledger ID column is hidden by default, but you can display it from the View Columns menu. If you enter multiple ledgers for the same run name, all of the ledgers must share the same chart of accounts.
BUDGET_NAME	Enter the appropriate budget name value for the budget line. You define the budget names in the Accounting Scenario value set.
PERIOD_NAME	Enter the period name that you're loading the budget data for. You can load budget data to Never Opened, Future Enterable, and Open periods only.
CURRENCY_CODE	Enter the currency for the budget.
SEGMENT1 to SEGMENT30	Enter valid and enabled account values for each segment in the chart of accounts.
BUDGET_AMOUNT	Enter the amount in the ledger currency for account types, expense and assets.
OBJECT_VERSION_NUMBER	For Oracle Cloud implementations, leave this field blank as the application automatically populates this when you load the data from the secure FTP server. For other implementations, you can set the column to a value of 1.

These columns remain blank because the budget import process either uses these columns for internal processing, or doesn't currently use them.

- CHART_OF_ACCOUNTS_ID
- CODE_COMBINATION_ID

- ERROR_MESSAGE
- CREATION_DATE
- CREATED_BY
- LAST_UPDATE_DATE
- LAST_UPDATE_LOGIN
- LAST_UPDATED_BY
- REQUEST_ID
- LOAD_REQUEST_ID

Related Topics

- Overview of External Data Integration Services for Importing Data

Budget Import to Budgetary Control

Load Budgets

You can load your enterprise-wide budget, including revenues and expenses, to General Ledger for analysis and reporting.

If you implement Budgetary Control, you need to also load your expense budget to Budgetary Control to validate your spending against the budget. Budget can be loaded for any combination of budget segment values for which you have access to. Budget account combinations are different from the account combinations used in transactions and can be subject to different validations.

How budget can be loaded into Budgetary Control depends on the source budget type of the control budget. Budget loaded to certain control budgets can be synchronized with budget in General Ledger, reducing the need to separately loading it to General Ledger.

Budget Balance Sources

This table explains how budget can be loaded into Budgetary Control and whether they're synchronized with General Ledger based on the source budget type and processing type.

Source Budget Type	Control Budget Processing Type	Methods of Loading Budget Balances	Synchronize Budget Balances from Budgetary to General Ledger
EPM Financials Module See Set Up Financials Cloud for Loading Budget from EPM.	Procure to pay	• Enter Budget in EPM using Planning and load using Data Exchange • Revise budget in EPM using Budget Revisions and load it using the Funds Reservation action	• Yes

Source Budget Type	Control Budget Processing Type	Methods of Loading Budget Balances	Synchronize Budget Balances from Budgetary to General Ledger
Hyperion Planning Can be reclassified to EPM Financials module See Set Up Oracle Fusion Financials for Loading Budget from EPM	Procure to pay	• Enter budget in EPM using Planning and load it using Data Exchange • Load budget with File Based Data Interface (FBDI) • Enter budget using Enter Budgets in Spreadsheet task • Enter budget transfer using Budget Transfer from the Review Budgetary Control Balances page	• No (if loaded from EPM or use Budget Transfer) • Yes (optional, if use FBDI or Enter Budgets in Spreadsheet)
Project Management	Procure to pay	Enter budget in Project Management and load it during budget baseline	• Not Applicable
Other Can be reclassified to EPM Financials Module when Allow funding from revenue option is disabled	Procure to pay	• Enter budget in a third-party software and load it using FBDI • Enter budget using Enter Budgets in Spreadsheet task • Enter budget transfer using Budget Transfer from the Review Budgetary Control Balances page • Automatically from Create Budget Entry from Revenue Process when Allow funding from revenue option is enabled	• Yes, optional
Other	Cash	• Enter budget in a third-party software and load it using FBDI • Enter budget using Enter Budgets in Spreadsheet task • Enter budget transfer using Budget Transfer from the Review Budgetary Control Balances page • Receivables receipt	No
Control Budget Control budget of this type is known as summary control budget and is linked to a control budget of one of the above source budget types	Procure to pay	Automatically updated in the summary control budgets when the budget balances are imported to the source detail control budget.	• Not Applicable
No Budget	Procure to pay	Budget can't be loaded	Not Applicable

Source Budget Type	Control Budget Processing Type	Methods of Loading Budget Balances	Synchronize Budget Balances from Budgetary to General Ledger
Used to track transaction spending, not spending against budget amounts			

Budget Balance Classifications

Budgetary Control can maintain and report budget balances separating initial budget from budget adjustments. This table explains how these two budget balance classifications are determined based on the methods of loading budget balances.

Methods of Loading Budget Balances	Budget Entry Classification
Load budget with File Based Data Interface (FBDI)	• Initial budget (if you specify budget entry classification as initial budget) • Budget adjustment (if you specify budget entry classification as budget revision)
Enter budget using Enter Budgets in Spreadsheet task	• Initial budget (if you specify budget entry classification as initial budget) • Budget adjustment (if you specify budget entry classification as budget revision)
Enter budget transfer using Budget Transfer form from the Review Budgetary Control Balances page	• Budget adjustment (always)
Enter Budget in EPM using Planning and load using Data Exchange when control budget's Source Budget Type is EPM Financial Module	• Initial budget (always)
Revise budget in EPM using Budget Revisions and load it using the Funds Reservation action	• Budget adjustment (always)
Enter budget in Project Management and load it during budget baseline	• Initial budget (if budget period is available for budgeting) • Budget adjustment (if budget period is open)
Receivables Receipt for cash budgets	• Budget adjustment (always)
Create Budget Entry from Revenue Process	• Initial budget (if you specify budget entry classification as initial budget) • Budget adjustment (if you specify budget entry classification as budget revision)

Related Topics

- Project and Grants Management
- Clear Budgetary Control Funds Check or Failures Requests
- Overview of Enterprise Performance Management
- Budgetary Control Validation of Receivables Receipts
- Automated Funding of Expense Budgets from Revenue

7 External Data Integration

Overview of External Data Integration Services for Importing Data

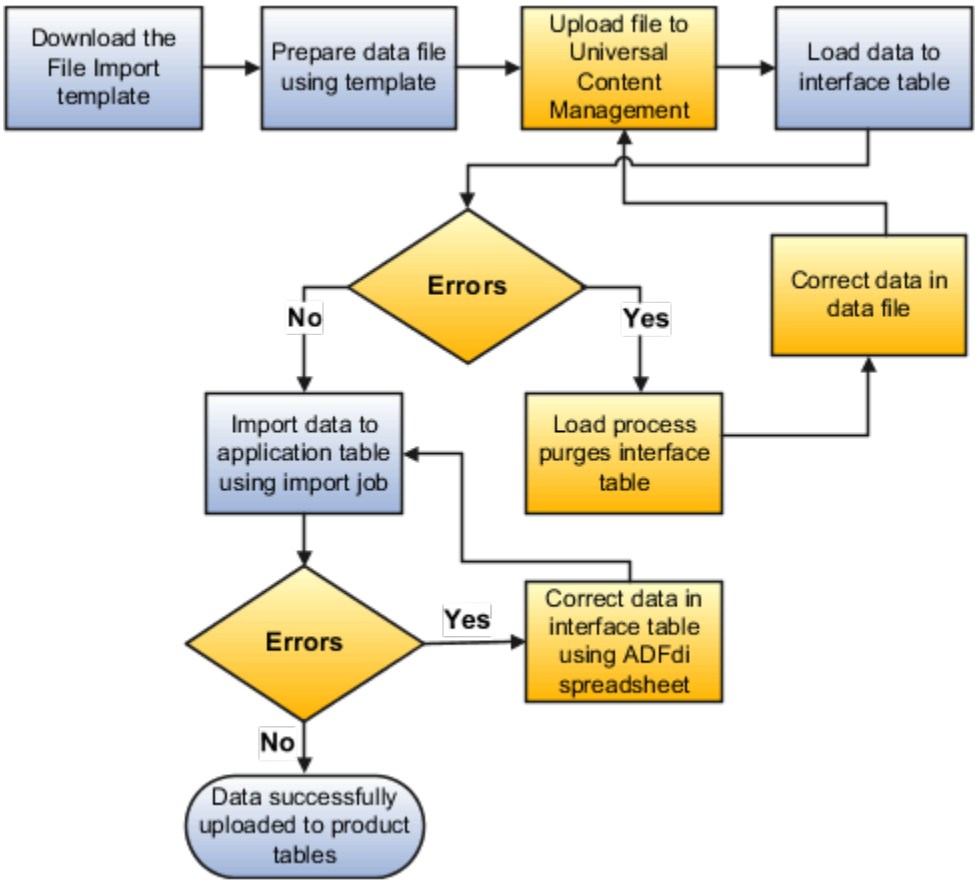
Use External Data Integration Services for Oracle Cloud to load data into the interface tables of Oracle Fusion Applications from external sources, such as legacy systems and third-party applications.

External Data Integration Services uses file-based data import (FBDI) templates and processes to import data.

The External Data Integration Services components consist of:

- Templates to structure, format, and generate the data file according to the requirements of the target application tables.
- File-based load process to load the data files into the interface tables.
- Application-specific data import processes to transfer data from interface tables to the application tables in your Oracle Fusion Applications.

The following flow diagram outlines the steps involved in loading data from external sources.



For further information, see Using External Data Integration Services for Oracle ERP Cloud (2102800.1) on My Oracle Support at **https://support.oracle.com**.

Related Topics

- Using External Data Integration Services for Oracle ERP Cloud

Considerations for Integrating with Financial External Systems

Oracle Fusion Applications provides:

- Flexibility for external systems integration.
- Many spreadsheets as an easy method for entering and loading key setup data into the applications.

The following are some of the ways you might use external system integration.

- Tax and conversion rates
- Payroll processing
- Bank statement reconciliation
- Budget preparation

Tax and Conversion Rates

Tax rates may vary depending on the geographical location of the customer or supplier, the type of product, and other factors.

- If your tax rates do not change frequently:
  - Enter or copy a tax rate feed of new or updated tax rates into the spreadsheet loader.
  - Upload the spreadsheet.

Note: Similar processes are used for foreign exchange conversion rates, which can change daily.

- Few foreign currency transactions: Use the spreadsheet loader.
- Many foreign currency transactions: Use a supplier for a direct load into the Daily Rates open interface. The application validates the rows in the interface table and then makes changes in the Daily Rates table.

Payroll Processing

If you are processing your payroll using an application other than Oracle Fusion Global Payroll:

- Use a spreadsheet template to load the data and create a postable journal entry in the Oracle Fusion General Ledger.
- Post the journal entry to reflect the payroll expense on your financial statements.

Set up the file from the payroll system to summarizes payments by cost center rather than detailed employee data. Summarized balances data is the level of detail relevant for the financial reporting and provides the confidentiality required for payroll information,

> **Note:** Oracle Fusion Financials marks the spreadsheet with clear error messages on the problematic rows, for example, a new cost center that must be setup, for ease of correction.

Bank Statement Reconciliation

Bank statements are often received daily and follow a fixed format. With Oracle Fusion Cash Management:

- Establish a transfer of the statements from the bank to the open interface.
- Run the automated process to load the bank statement file.
- Run the reconciliation process.

> **Note:** If there are any errors in the file, the reconciliation process stops. The load process indicates the errors so you can follow up with the bank and receive a corrected file.

Budget Preparations

There are two approaches to preparing your budgets:

1. For simple budgeting:
    - Distribute the current actual results and prior budget numbers to the relevant finance professionals using spreadsheets.
    - Collect and consolidate the spreadsheets.
    - Load the spreadsheets to the Essbase cube.
    - Compare actual results against budgets using all of the Oracle Fusion Financials reporting and analysis tools, including Account Monitor, Account Inspector, Smart View, and Financial Reporting.
2. For more complex budgeting use Oracle Hyperion Planning on the Oracle Cloud, alongside Oracle Fusion Financials. Advantages include:
    - Advanced tools to handle complex budgeting scenarios.
    - Direct flow of data between the two applications.
    - Simplified distribution and collection of budget data.

> **Note:** For more information on external data integration see: **Oracle Financials Cloud Implementing Common Features for Financials** guide: **External Integration** chapter: **External Data Integration Services for Oracle Cloud**.

8 Third-Party Integration

Embedded Banking Services

Embedded banking services provides your businesses with a comprehensive view of your financial position to operate your day-to-day business finance effectively.

Before using this feature, you must first work with your bank's implementation team to establish the bank accounts and the related scope of the services you want to include. Please contact your bank's sales/relationship manager.

> **Note:** This feature is currently in controlled availability and requires a promotion code. To inquire about the promotion code, log a service request through My Oracle Support. You'll need to provide the production pod names.

The solution provides integrated banking and payment services enabled from turnkey connectivity between Oracle Fusion Cloud ERP and your bank for U.S. and Canada customers. It includes synchronization of all bank account master data, the requisite setup needed to automate funds capture/disbursement, and continuous bank statement retrieval, processing, and reconciliation.

The integration also provides a seamless onboarding experience by automatically configuring connectivity and importing bank account master data.

Depending on your bank, the Banking Configurations functional area may support enablement of the following business flows:

- **Banks and Bank Accounts:** Configure security credentials and your bank, bank branches, and bank accounts automatically with Oracle Cloud ERP.
- **Funds Disbursement:** Configure payment and acknowledgment processing setups for disbursements. Process disbursements seamlessly with your bank.
- **Funds Capture:** Configure direct debit, acknowledgment and lockbox processing setups for receipts. Process receipts and lockbox seamlessly with your bank.
- **Bank Statement Processing:** Configure bank statement formats and reconciliation setups, and quickly process and reconcile your bank statements.

Connectivity and Bank and Bank Accounts

Manage banks, bank branches, and bank accounts using the integration with your bank. This maximizes efficiency and eliminates time-consuming activities through automated maintenance of bank accounts and related reconciliation configurations.

Depending on your bank, an onboarding file automatically generates the bank master data, while in other cases, you use a standard turnkey spreadsheet to create the bank accounts. Once the bank accounts are created, the process automatically attaches the business functions and business units, reconciliation configurations, and bank statement transaction creation rules needed for payables and receivables processing. Users can review the onboarded bank accounts from the bell notifications.

Funds Disbursement

Process payment and acknowledgment files for funds disbursement using the integration with your bank. Customers can generate and send payment files in the bank's preferred format and retrieve and process disbursement acknowledgment files.

The integration uses the bank's message format based on ISO20022 CGI standards. This format includes payment by ACH, Wire, and check for the US and Canada. It also supports SEPA payments for some banks, within the SEPA zone, which contains 27 member states of the EU, along with Iceland, Liechtenstein, Norway, Switzerland, the United Kingdom, Andorra, Monaco, San Marino, and Vatican City. The integration provides the acknowledgment processing feature with complete automation for file retrieval and processing. It processes L0, L1 and L2 acknowledgment files generated by your bank at various points in the clearing flow. The invoice status changes from Paid to Unpaid for rejected payments, allowing users to take corrective action. Users receive bell notifications indicating the successful completion or failure of the payment batch and acknowledgment processing.

The Funds Disbursement flow also allows generation of the positive pay file for the checks printed in-house by customers, and the output is in XML format.

Funds Capture - Direct Debit Processing

Process direct debit settlement batch and acknowledgment files using the integration with your bank. Customers can generate and send direct debit settlement batch files in the bank's preferred format and retrieve and process direct debit disbursement acknowledgment files.

The integration uses the bank's message format based on ISO20022 CGI standards. This format includes ACH direct debits for the US and Canada. The integration provides the acknowledgment processing feature with complete automation for retrieval and processing of bank acknowledgment files. It either processes L0, L1, and L2 acknowledgment files, or file-level and transaction-level acknowledgment files, generated by your bank at various points in the clearing flow. The receipt status changes from Remitted to Confirmed for rejected settlements, allowing users to take corrective action in Receivables. See *How Receipts are Reversed* for more information. Users receive bell notifications indicating the successful completion or failure of settlement batch and acknowledgment processing.

Funds Capture – Lockbox

Process intraday lockbox using the integration with your bank to enable near real-time customer balances. Your bank can provide a remittance service that includes payment advice processing and remittance advice collection from emails and Excel files. Payment advice and remittance information are collated and combined with the lockbox file, eliminating the need for manual entry and application.

Bank Statement Processing

Process and reconcile bank statements using the automated integration with your bank. This maximizes efficiency, uses real-time bank balances, and eliminates time-consuming activities through automatic bank statement processing and reconciliation.

The integration uses the bank's CAMT053 bank statement template, based on ISO20022 standards. The use of this template enables seamless bank statement file retrieval and processing. Features include:

- Regular retrieval and processing of prior day bank statements
- Automatic creation of new bank statement transaction codes reported on bank statement lines
- Automatic creation of bank statement transaction creation rules and reconciliation of bank statement lines
- Automatic unreconciliation and voiding of rejected payments, and reconciliation of the original and rejected bank statement lines

- Automatic reversal of rejected direct debit transactions and reconciliation of reversal bank statement lines
- Automatic generation of bell notifications to confirm completion of the automatic reconciliation process, including reconciliation exceptions, if any

Real-Time Account Balance Processing

Apply ready-to-use integration with the bank to retrieve real-time account balances and alert users during transaction processing for shortfalls.

Real-time balances are retrieved and displayed only for bank accounts with prior-day bank statements.

Related Topics

- Use Promotion Codes

Which embedded banking features are offered by the participating banks?

Supported embedded banking features vary by participating bank, as noted below.

	J.P. Morgan	PNC	Bank of America
Connectivity	Yes	Yes	Yes
Funds Disbursement	• US/Canada: ACH, Wire, Outsourced Check Printing • Eurozone + UK (EUR only): SEPA • All other countries - contact bank	• US/Canada: ACH, Wire	• US/Canada: ACH, Wire, Outsourced Check Printing • Eurozone + UK (EUR only): SEPA • All other countries - contact bank
Funds Disbursement - Positive Pay	Yes	Yes	
Funds Capture - Lockbox	Yes	Yes	Yes
Funds Capture - Direct Debit	Yes		
Bank Statement Processing	Yes	Yes	Yes
Real-Time Balance	Yes		

Bank Account Validation Service

Bank account validation service is a paid service provided by partner banks to ensure that supplier bank account details are correct and valid.

The Bank Account Validation checks the following:

- Bank account validity to ensure it exists and is valid.
- Bank account owner authentication to confirm that the bank account belongs to the supplier being registered.

The verification status includes the verification outcome of both the bank account validity and the bank account owner authentication. Based on the outcome of both checks, a final status and supporting message is displayed to the approvers. These are the possible statuses for bank account verification.

Status	Meaning
Verified	Bank account is open, valid, and the supplier is the account owner.
Failed	• Bank account is invalid or currently closed for payment transactions, and the account owner couldn't be validated. • Bank account is open and valid, but the supplier isn't the account owner.
Inconclusive	Bank account details couldn't be validated because the account couldn't be found and the account owner couldn't be validated.

Note: The status of the bank account verification is informational only, and doesn't prevent further processing in the system.

Related Topics

- Bank Account Validation Services Questions and Answers

Touchless Expenses with J.P. Morgan Corporate Cards

The new generation mobile experience with J.P. Morgan corporate cards delivers touchless expense submission and faster reimbursement.

Receive instant alerts when charges are incurred on J.P. Morgan corporate cards. Use guided correction, intelligent recommendations, and correct receipt extraction to ease automatic expense submission and approval. Automatically extract expense attributes from expense receipts in multiple languages using the Document IO agent. Available to customers with J.P. Morgan corporate cards.

Note: This feature is currently in controlled availability and requires a promotion code. To inquire about the promotion code, log a service request through My Oracle Support. You'll need to provide the production pod names and the business units that will be using Touchless Expenses.

The Touchless Expenses application is ideally suited for large companies looking to simplify their expense workflow processes and reimbursement policies.

Key functionality of Touchless Expenses include:

- AI-Powered Expense Policy Inquiry Using Expenses Policy AI Agent
- Real-time expense creation with J.P. Morgan corporate cards.

- Guided help for expenses that require more information.
- Automatic submission of completed expenses.
- Intuitive user interface and application experience.

AI-Powered Expense Policy Inquiry Using Expenses Policy AI Agent

Use the Expenses Policy AI agent to provide quick, contextual answers to employees' corporate travel and expenditure policy questions. You can also leverage the agent to help answer other questions related to the Touchless Expenses application.

Upload the organization's expense policies directly into the system. Employees can then query the agent to understand key policy details before incurring business expenses or submitting claims.

To use this feature, at least one business unit must be enabled with *Touchless Expenses with J.P. Morgan Corporate Cards*.

> **Note:** Watch a quick demo of this feature for reference: *Expense Policy Inquiry Using Expense Policy Agent for Touchless Expenses with J.P. Morgan Cards*.

Get Started with the Expenses Policy Agent

To get started with the Expenses Policy Agent, you'll need to upload at least one document. Here's how:

1. Go to Setup and Maintenance.
2. Search for **Manage Expenses System Options**.
3. Find and open **Document for Expenses Policy Agent**.
4. Upload your policy and FAQ documents as needed.

   > **Note:** Fusion Applications provides a *Touchless Expenses user application manual and FAQ* that serves as a baseline document. It's recommended that you modify it before uploading it to the Expenses Policy Agent, especially sections that need to be tailored to customer-specific information such as e-receipt forwarding address. Download the document and edit it before using.

   Uploaded documents must be in PDF, .txt, MS Word, or .html format. For best results, follow the agent best practices linked below. If your documents include complex tables or images, convert them to plain text. See *Author Documents to Maximize Answer Accuracy - Document Content* for details.

   You can upload multiple documents at once. To prevent conflicting information across files, be sure to follow the best practices for handling multiple documents. See *Author Documents to Maximize Answer Accuracy - Document Structure* for details.
5. Save your changes.

Once a document is uploaded, the **Expenses Policy Agent** option becomes available for Touchless Expenses users in the overflow menu of the application.

Uploaded documents will be used by all Touchless Expenses users across every business unit.

Update a Policy Document

1. Go to the existing document for Expenses Policy Agent.
2. Remove the old document and click **Save**.

3. Upload the new one and save your changes.

Configure Prompts

Fusion Applications offer the capability for you to tailor the prompt to meet your specific needs. See *Can I configure my own prompts for the Expenses Policy Agent?* for more information.

Real-time Expense Creation with J.P. Morgan Corporate Cards

Touchless Expenses users benefit from real-time expense creation when they incur charges on a J.P. Morgan corporate card.

When users incur charges on their J.P. Morgan corporate card, Touchless Expenses instantaneously creates the expenses and notifies the user on their mobile device, clearly identifying the expenses requiring more information. Users can click the notification to provide the missing information.

These corporate card expenses remain in the application with a "Pending final charge" status until the settled charge arrives. The status is removed and the expense is now ready for submission if no other information is required. Users see a message: "Final charge posted" at the top of the expense indicating the settled charge has arrived.

Guided Help for Expenses that Require More Information

Expense users follow guided prompts to quickly provide information for incomplete expenses. For example, in some instances, expenses might require more user input to comply with company policies. There are two ways to access the guided help: from the notification on the user's mobile device or from within the Touchless Expenses application. When an expense user receives a notification on their mobile device after a corporate card charge is incurred, they select the notification which directs them to a guided experience to complete the expense. From within the application, the user selects the message on the top of the landing page indicating action is required on one or more expenses. The guided help provides clear instructions on how to fill in the required information. This allows users to complete their expenses easily and as soon as they're incurred.

The guided help supports the following common scenarios:

- Expenses missing simple fields such as expense type, amount, and currency.
- Expenses that require receipt or missing receipt justification.
- Expenses missing more information such as number of attendees and attendee names.
- Expenses violating corporate policies such as amount limits and card usage.
- Potential duplicate expenses.

Automatic Submission of Completed Expenses

Automatic submission allows the user to set up a specific day of the week to have their expenses compiled into a report and submitted for approval. The company administrator configures this for each business unit and identifies which days of the week are available for employees to select for automatic submission, after which employees can turn on auto submission from the Settings page. On the selected automatic submission day, the Touchless Expenses application compiles all eligible expenses into a single report and submits them for approval. Any expenses that require more information remain in the application and aren't automatically submitted. By enabling automatic submission, the expense user's experience can be fully automated from expense creation to submission.

Intuitive User Interface and Application Experience

Touchless Expenses supports policy enforcement, configuration for company-specific information, attendee capture, and various types of default values. The application is simplified into four main pages: expense landing page, manual expense creation page, search page, and settings page. It also provides employees with a seamless first-time user experience.

Related Topics

- Use Promotion Codes