Oracle® Monetization Cloud

Security Guide

Release 18B

E92622-02

August 2018

Oracle Monetization Cloud Security Guide, Release 18B

E92622-02

Contents

Preface

1 About Oracle Monetization Cloud security

2 Getting started with User Management

3 Implementing role-based application security

Preface

This document provides guidelines for managing security in Oracle Monetization Cloud.

Audience

This document is intended for anyone involved in implementing and administering security for Oracle Monetization Cloud.

Documentation Accessibility

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

Access to Oracle Support

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

1
About Oracle Monetization Cloud security

Oracle Monetization Cloud is secured by you and by Oracle. You protect the service by using roles to control which environments and functionality users can access and by configuring secure integrations with external applications. Oracle protects your data by implementing internal security measures.

Topics in this document

About role-based application security

In Oracle Monetization Cloud, a user's access to environments and functionality is determined by the roles assigned to the user. See Implementing role-based application security.

About integrating external applications securely

To securely integrate external applications with Oracle Monetization Cloud, you can do the following:

- Configure Oracle Monetization Cloud to use an external Security Assertion Markup Language (SAML) identity provider to authenticate access requests for operations such as single sign-on through a customer relationship management (CRM) system. See Using SAML to authenticate access requests.
- Register external applications as OAuth clients to authorize them to call Oracle Monetization Cloud web services. See Using OAuth to authorize access.
- Import Secure Sockets Layer (SSL) certificates to secure connections between Oracle Monetization Cloud and external service providers, such as payment processors and tax calculators. See Using SSL to secure connections to service providers.
- Use secure file transfer protocol (SFTP) to protect data as you upload and download files between Oracle Monetization Cloud and external systems. See Transferring files securely with SFTP.

About data privacy in Oracle Monetization Cloud

Oracle Monetization Cloud helps protect private data by:

- Encrypting data in and connections to the database. See Encrypting data.
- Purging unneeded customer data. See Purging data.

- Masking personal data for roles that don't need it. See Masking data in logs.
- Restricting access to UIs that expose personal data based on user roles. See Implementing role-based application security.

You can support data privacy by:

- Understanding how your payment and taxation gateways handle personal data.
- Assigning users only the roles they need to perform their tasks. For example, a pricing analyst doesn't need to see a customer's address or credit card number, and so doesn't need access to Subscriber Management.
- Gaining verbal consent from your customers to enter and store their personal data.
- Immediately removing customers' personal data if requested.

Oracle Monetization Cloud complies with Oracle hosting and delivery policies, including use of encrypted connections, security (network, data, access, and configurations), high availability, and disaster recovery.

For more information, see *Oracle Online Cloud Services Agreement*, available on the Oracle Cloud Services contracts page:

`http://www.oracle.com/us/corporate/contracts/cloud-services/index.html`

Related topics

- Implementing role-based application security
- About data privacy
- About integrating your business systems

2
Getting started with User Management

Create and manage accounts, assign roles, and control access privileges for Oracle Monetization Cloud.

Important:

- To avoid losing data, do not use browser commands such as **Back**, **Forward**, and **Refresh**.
- Ensure that cookies are enabled in your browser.

Topics in this document

- Creating and removing users
- Assigning roles
- Setting up access privileges

Creating and removing users

Use Oracle Identity Manager to create and remove user accounts. See:

- Creating users in Oracle Monetization Cloud
- Removing users from Oracle Monetization Cloud

Assigning roles

Use Oracle Identity Manager to assign roles to your system's users for accessing Oracle Monetization Cloud environments and applications. You can't modify the preconfigured Oracle Monetization Cloud roles or create new roles. See:

- About implementing role-based application security for Oracle Monetization Cloud
- Assigning roles to users in Oracle Monetization Cloud

You can also review and change role assignments.

Setting up access privileges

Use Oracle Entitlements Server to control access privileges for the Oracle Monetization Cloud home page and these applications:

- Subscriber Management
- Business Operations Center

See:

- Changing the default limits for Subscriber Management roles
- Oracle Entitlements Server Help

3

Implementing role-based application security

This document explains how to implement role-based application security for Oracle Monetization Cloud.

Topics in this document

See also:

- Information about roles and users in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- Information about managing password policies in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

About implementing role-based application security for Oracle Monetization Cloud

Oracle Monetization Cloud comes with a preconfigured set of roles. You manage access to Oracle Monetization Cloud environments and functionality by assigning those roles to users.

> **Note:**
>
> You can't create or modify roles. You can, however, mix and match existing roles among users to create unique combinations of environment and functional access for each user.

You must assign the following types of roles to each user:

- One or more environment roles

Environment roles grant access to your Oracle Monetization Cloud development and production environments. See Environment roles in Oracle Monetization Cloud .

- One or more functional roles

  Functional roles determine which applications a user can access from the Oracle Monetization Cloud home page and which operations the user can perform in those applications. See Functional roles in Oracle Monetization Cloud .

All of a user's functional roles are valid for each environment the user has access to. A user can't have a different set of functional roles for different environments. This means, for example, that you can't grant a user access to Offer Design in your development environment but deny the user access to Offer Design in your production environment.

For more information, see the discussion about managing roles in *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*.

Environment roles in Oracle Monetization Cloud

The following table lists the environment roles available in Oracle Monetization Cloud:

Environment Role	Description
Development	Grants access to your development Oracle Monetization Cloud instance
Production	Grants access to your production Oracle Monetization Cloud instance

Functional roles in Oracle Monetization Cloud

Access to most Oracle Monetization Cloud functionality requires two types of functional roles:

- Roles that grant access to the appropriate applications on the Oracle Monetization Cloud home page
- Roles that grant access to application or system administration functionality

For example, to have read/write access to Offer Design, a user needs the following functional roles:

- **Pricing Analyst:** Grants access to Offer Design on the Oracle Monetization Cloud home page
- **Pricing Design Admin:** Grants read/write access to Offer Design

To maintain data privacy and security, assign users only the roles they need to accomplish their tasks, especially for roles that expose customer personal data. For example, a system administrator doesn't need to see customer contact information to configure event messaging, and a pricing analyst doesn't need to see customer invoices to analyze new offerings, so neither of these users need access to Subscriber Management.

The following sections list the functional roles available in Oracle Monetization Cloud:

- Functional roles for accessing applications
- Business Configuration functional roles

- Business Operations functional roles
- Offer Design functional roles
- Oracle BI Publisher functional roles
- Subscriber Management functional roles
- System administration functional roles

Functional roles for accessing applications

The functional roles in the following table grant access to the specified applications from the Oracle Monetization Cloud home page. To access application functionality, users need additional functional roles (see the following sections).

> **Note:**
>
> If a user doesn't have a role that grants access to an application, a "no authorization" message appears when the user opens the application.

Application access functional role	Description
BRM Admin	Grants read-only access to the following applications: • **Subscriber Management** To access the application, users must also have a role listed in Subscriber Management functional roles. • **Oracle BI Publisher** To access the application, users must also have a role listed in Oracle BI Publisher functional roles. Grants access to **Business Configuration**. This role enables users to set up prerequisite configurations used to design product offerings, to create accounts, to run billing, and to perform other functions. See also Business Configuration functional roles.
CSR	Grants read-only access to the following application: • **Subscriber Management** To access the application, users must also have a role listed in Subscriber Management functional roles.
Financial Analyst	Grants read-only access to the following applications: • **Subscriber Management** To access the application, users must also have a role listed in Subscriber Management functional roles. • **Business Operations** To access the application, users must also have a role listed in Business Operations functional roles. • **Oracle BI Publisher** To access the application, users must also have a role listed in Oracle BI Publisher functional roles. Grants access to **Business Configuration**. This role enables users to create tax codes, general ledger accounts, and other business-related components. See also Business Configuration functional roles.

Application access functional role	Description
Operations	Grants read-only access to the following applications: • **Subscriber Management** To access the application, users must also have a role listed in Subscriber Management functional roles. • **Business Operations** To access the application, users must also have a role listed in Business Operations functional roles.
Pricing Analyst	Grants read-only access to **Subscriber Management**. To access the application, users must also have a role listed in Subscriber Management functional roles. Grants access to **Offer Design**. This role enables users to create and edit pricing components and to review setup components. See also Offer Design functional roles.
Sys Admin	Grants read-only access to the following applications: • **Oracle Identity Self Service** in **User Management**. To manage their own Oracle Monetization Cloud account, users must also have the OIMAdministrators functional role. To perform administrative functions in Oracle Access Manager and Oracle Identity Manager, users must also have the IDM Administrators role. • **Oracle Entitlements Server** in **User Management** To create application access policies, users must also have the OESAdministrators role. See System administration functional roles. Grants read/write access to the following applications: • **Event Publishing** in **System Configuration**. This role enables users to configure Oracle Monetization Cloud for event publishing and email messaging. See Sending data to external applications and Sending messages to customers. • **Payment Gateway** in **System Configuration** This role enables users to connect Oracle Monetization Cloud to external payment gateways. See Connecting to payment gateways. • **Taxation Gateway** in **System Configuration** This role enables users to connect Oracle Monetization Cloud to external taxation gateways. See Connecting to taxation gateways. • **SSL Certificate** in **System Configuration** This role enables users to import Secure Sockets Layer (SSL) certificates to secure connections between Oracle Monetization Cloud and external service providers, such as payment processors and tax calculators. See Using SSL to secure connections to service providers. • **Federation Services** in **System Configuration** This role enables users to configure the following: External Security Assertion Markup Language (SAML) identity providers to authenticate requests for access to web services. See Using SAML to authenticate access requests. OAuth clients to authorize external applications to access web services. See Using OAuth to authorize access.

Business Configuration functional roles

The roles listed in the following table grant functional access to Business Configuration.

> **Note:**
>
> To work with Business Configuration, users need one of the roles listed below and either the BRM Admin or Financial Analyst functional role described in Functional roles for accessing applications.

Business Configuration functional role	Description
BRM Admin	Enables users to set up prerequisite configurations used to design product offerings, to create accounts, to run billing, and to perform other functions.
Financial Analyst	Enables users to create tax codes, general ledger accounts, and other business-related components.
DesignCenterAdapterGroup	This role is required to submit changesets in Business Configuration.
JDGroup	This role is required to submit changesets in Business Configuration.

Business Operations functional roles

The roles listed in the following table grant functional access to Business Operations.

> **Note:**
>
> To work with Business Operations, users need one of the roles listed below and either the Financial Analyst or Operations functional role described in Functional roles for accessing applications.

Business Operations functional role	Description
BOC_SUPER_ADMIN	Enables users to access all Business Operations functionality.
OPERATIONS_VIEW	Gives users read-only access to Business Operations functionality, including job history and log files..
FINANCIALS_VIEW	Enables users to view business metrics on the Business Dashboard page.
OPERATIONS_BILLING_ADMIN	Enables users to manage billing jobs, including scheduling jobs, modifying them, and viewing their history.
OPERATIONS_FINANCE_ADMIN	Enables users to manage jobs for general ledger, payment collections, invoicing, and refunds, including scheduling jobs, modifying them, and viewing their history.
OPERATIONS_PRICING_SYNC_ADMIN	Enables users to manage product catalog synchronization jobs, including scheduling jobs, modifying them, and viewing their history.

Offer Design functional roles

The roles listed in the following table grant functional access to Offer Design.

Note:

To work with Offer Design, users need one of the roles listed below and the Pricing Analyst functional role described in Functional roles for accessing applications.

Offer Design functional role	Description
Pricing Design Admin	Grants read/write access to all pricing and setup components in Offer Design.
Pricing Analyst	Grants read/write access to all pricing components and read-only access to all setup components in Offer Design.
Pricing Reviewer	Grants read-only access to all pricing and setup components in Offer Design.
DesignCenterAdapterGroup	This role is required to submit changesets in Offer Design.
JDGroup	This role is required to submit changesets in Offer Design.
MigrationAdmin	Enables users to migrate pricing data from the Oracle Monetization Cloud database to the Offer Design database.

Oracle BI Publisher functional roles

The roles listed in the following table grant functional access to Oracle BI Publisher.

Note:

To work with Oracle BI Publisher, users need one of the roles listed below and either the BRM Admin or Financial Analyst functional role described in Functional roles for accessing applications.

Oracle BI Publisher functional role	Description
BIAdministrators	Enables users to manage Oracle BI Publisher application settings.
BIReportAdministrators	Grants read/write access to all reports and templates in the system, including those created by other users.
BIAuthors	Grants read/write access to the user's reports and templates.
BIConsumer	Grants read-only access to reports and templates created by other users.

Subscriber Management functional roles

The roles listed in the following table grant functional access to Subscriber Management.

Because Subscriber Management exposes customer personal data, such as contact and financial information, we recommend only granting these roles to the users who truly need them to accomplish their tasks. This helps promote data privacy.

> **Note:**
>
> To work with Subscriber Management, users need one of the roles listed below and either the BRM Admin, CSR, Financial Analyst, Operations, or Pricing Analyst functional role described in Functional roles for accessing applications.

Subscriber Management functional role	Description
Regular CSR	Grants read/write access to subscribers' payments and adjustments up to a specified amount. By default, this role has the following limits, which are specified as units of a balance (for example, in US dollars, 30 units equals $30.00, and in minutes, it equals 30 minutes): • Maximum noncurrency adjustment amount: 40 • Maximum currency adjustment amount: 30 • Maximum payment amount: 50 To change these limits, see Changing the default limits for Subscriber Management roles.
Super CSR	Grants read/write access to all subscriber information.
ReadOnly	Grants read-only access to all subscriber information.
WriteOff	Enables users to write off unpaid or disputed accounts receivable.
AccountResource	Enables users to perform the following tasks: • Create accounts. • Search for accounts. • Change account status. • View account profiles and other customer information. Prevents users from adding, deleting, or saving contact information.
PaymentResource	Enables users to perform the following tasks: • Make payments. • Move posted payments into suspended status. • Reverse payments. • Allocate payments. • Allocate suspended payments partially or fully to an account. • View audit information in the payment details screen. (Audit information in the payment suspense screen is always visible.) • Make batch payments. • Reverse suspended payments. Prevents users from performing the following tasks: • Viewing general payment suspense information. • Making suspended payments. • Assigning and reassigning suspense payment handlers to suspended payments.
RefundResource	Enables users to refund payments. By default, the maximum refund amount that this role can issue is 3 units of a balance (for example, in US dollars, 3 units equals $3.00). To change the maximum refund amount, see Changing the default limits for Subscriber Management roles.

Changing the default limits for Subscriber Management roles

To change the default limits in Subscriber Management roles:

1. Open the User Management application.
2. Select **Oracle Entitlements Server**.
3. Under **Authorization Policies**, select **Search**.
4. In the Search section, select **Search**.
5. In the Search Results table, select the row that corresponds to the role whose limits you want to change.

   For example, for the Regular CSR role, select the **Regular CSR Policy** row.
6. Select **Open**.
7. In the Targets table, select the target that corresponds to the limit you want to change.
8. Select the **Obligations** tab.
9. In the Attributes table, select the appropriate attribute.
10. Select **Edit**.
11. In the Edit Obligation Attribute dialog box, change the value.
12. Select **Update**.
13. Select **Apply**.

System administration functional roles

The roles listed in the following table grant access to various Oracle Monetization Cloud system administration functions.

> **Note:**
>
> To work with the system administration applications, users need one of the roles listed below and the Sys Admin functional role described in Functional roles for accessing applications.

System administration functional role	Description
IDM Administrators	Enables users to perform Oracle Identity Manager administrative functions.
OIMAdministrators	Enables users with access to **Oracle Identity Self Service** in **User Management** to manage their own Oracle Monetization Cloud account as follows: • Manage their profile, passwords, challenge questions, direct reports, and proxies. • View resources they have access to. • Request access to additional resources. • Track the status of their pending requests. • Perform fulfillment tasks assigned to them. • Respond to approval requests assigned to them.

System administration functional role	Description
OESAdministrators	Enables users to control access privileges for the following by using Oracle Entitlements Server: • Subscriber Management • Business Operations Center • Oracle Monetization Cloud home page For more information, see the Oracle Entitlements Server online Help.
SOAP Administrator	Grants administrative access to the Oracle Monetization Cloud SOAP API.
WSIntegration	For use when basic authentication of SOAP requests is required. Enables an integration user to perform tasks from a SOAP client or integration using the Oracle Monetization Cloud SOAP API.

About Oracle Monetization Cloud users

Oracle Monetization Cloud includes one default administrative user, *TenantSysAdmin*.

> **Note:**
>
> In this topic, *TenantSysAdmin* is a placeholder for the name you give your default administrative user when your Oracle Monetization Cloud system is set up.

This is the only user who can manage the other users needed for your Oracle Monetization Cloud environments. User management tasks include:

- Creating, disabling, and deleting users
- Assigning, removing, and viewing roles
- Resetting passwords

In addition to user management capabilities, the *TenantSysAdmin* user has the following roles that enable other administrative functions:

- Production
- Sys Admin
- IDM Administrators
- OESAdministrators
- OIMAdministrators

For more information about users and roles, see the following topics:

- Creating users in Oracle Monetization Cloud
- Environment roles in Oracle Monetization Cloud
- Functional roles in Oracle Monetization Cloud

About Oracle Monetization Cloud test users

In addition to *TenantSysAdmin*, Oracle Monetization Cloud includes the test users that Oracle uses to set up Oracle Monetization Cloud.

After setup, Oracle disables and locks the test users, but they remain visible in the Oracle Identity Manager **Users** tab. You can display their details by selecting their names.

> **Note:**
>
> Don't unlock and reenable the test users. Instead, use them as *examples* to guide you in creating your own users.

The following table lists the Oracle Monetization Cloud test users and their roles:

Test user	Roles
SysAdmin	Sys Admin IDM Administrators OESAdministrators OIMAdministrators
BRMAdmin	BRM Admin CSR Regular CSR Super CSR BIAdministrators BIAuthors BIConsumer DesignCenterAdapterGroup
FinancialAnalyst	Financial Analyst CSR Regular CSR BOC_OPERATIONS_FINANCE BIAdministrators BIAuthors BIConsumer DesignCenterAdapterGroup

Test user	Roles
PricingAnalyst	CSR Regular CSR Super CSR Pricing Analyst Pricing Reviewer Pricing Design Admin DesignCenterAdapterGroup JDGroup MigrationAdmin
CSR	CSR Regular CSR Super CSR ReadOnly AccountResource PaymentResource RefundResource WriteOff
Operations	Operations Super CSR BOC_OPERATIONS_ADMIN
soapUser	SOAP Administrator

Creating users in Oracle Monetization Cloud

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

You can assign roles to users when you create the users, or you can assign roles later.

For a list of roles that you can assign to users, see the following sections:

- Environment roles in Oracle Monetization Cloud
- Functional roles in Oracle Monetization Cloud

> **Caution:**
>
> Oracle recommends that you carefully consider Oracle Monetization Cloud security when creating users and assigning roles. Create unique users for each environment and assign each user only the functional roles required for the user to perform his or her assigned tasks.

To create a user:

1. Open the User Management application.

2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.
4. Select **Users**.
5. Select **Create**.
6. Enter the user information. The following table lists the minimum recommended fields. Use additional fields as needed for your business requirements.

Fields	Description
Effective Date	Specify the effective date of the new user account.
Justification	Specify the justification for the new user account.
Basic Information	Includes the **Name**, **E-mail**, **Organization**, and **User Type** fields. Oracle provides a default organization for your Oracle Monetization Cloud environment. Select the magnifying glass icon next to the **Organization** field to select your organization value.
Account Settings	Includes the **User Login** and **Password** fields. Select the icon next to the **Password** field to display password requirements. New users must change their passwords the first time they sign in. For information about the default password policy, see Setting password policies for Oracle Monetization Cloud.

7. Select **Submit**.

   The **Users** tab appears.
8. Select **Refresh**.

   The new user appears in the Users table.
9. Select the new user's sign-in name.

   The new user's details tab appears.
10. Select the user's **Roles** tab.
11. Select **Request Roles**.

    The **Role Access Request** tab appears. Use this tab to assign environment and functional roles to the new user.

Assigning roles to users in Oracle Monetization Cloud

You can assign roles to Oracle Monetization Cloud users in either of the following ways:

- Assign roles as you create a user. See Creating users in Oracle Monetization Cloud.
- Assign roles after a user is created. See Assigning roles to existing users in Oracle Monetization Cloud.

Assigning roles to existing users in Oracle Monetization Cloud

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

For a list of roles that you can assign to users, see the following sections:

- Environment roles in Oracle Monetization Cloud
- Functional roles in Oracle Monetization Cloud

> **Caution:**
>
> Oracle recommends that you carefully consider Oracle Monetization Cloud security when assigning roles. Assign each user only the functional roles required for the user to perform his or her assigned tasks.

To assign a role to an existing user:

1. Open the User Management application.
2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.
4. Select **Users**.

   The **Users** tab appears.
5. Use the **Search** fields to find the user you want to assign a role to.

   Users meeting the search criteria are listed in the search results.
6. In the **User Login** column, select the link for the user you want to assign a role to.

   The **User Details** tab appears.
7. Select the **Roles** tab if it's not open by default.
8. Select **Request Roles**.

   The **Role Access Request** tab appears.
9. In the **Catalog** tab, select the roles you want to assign:
   - To select an individual role, select the role's **Add to Cart** icon.
   - To select multiple roles, use the **Ctrl** key, and then select **Add Selected to Cart**.

   For a list of available roles, see the following sections:
   - Environment roles in Oracle Monetization Cloud
   - Functional roles in Oracle Monetization Cloud
10. Select **Checkout** at the top of the **Role Access Request** tab.
11. (Optional) Enter a justification and an effective date.
12. Select **Submit**.

13. Select **Refresh**.

    The new roles appear in the user's list of roles.

Reviewing roles and role assignments in Oracle Monetization Cloud

You can view the following information about roles in Oracle Monetization Cloud:

- All roles assigned to a specific user. See Viewing the roles assigned to a user.
- All users who have a specific role. See Viewing all users who have a specific role.
- All available roles. See Viewing all available roles.

Viewing the roles assigned to a user

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To view the roles assigned to a user:

1. Open the User Management application.
2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.
4. Select **Users**.

   The Users tab appears.
5. Use the **Search** fields to find the user whose roles you want to view.

   Users meeting the search criteria are listed in the search results.
6. In the **User Login** column, select the link for the appropriate user.

   The User Details tab appears.

   In the User Details tab, the Roles tab is open by default. A list of all the roles assigned to the user is displayed in the tab.

   For information about roles, see Environment roles in Oracle Monetization Cloud and Functional roles in Oracle Monetization Cloud .

Viewing all users who have a specific role

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To view all users who have a specific role:

1. Open the User Management application.
2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.

4. Select **Roles**.

   The **Roles** tab appears.

5. Select the name of the appropriate role.

   The role's tab appears.

6. Select the **Members** tab.

7. In the tab's **Member assignment** table, select **All Members**.

   All users assigned to the role are listed in the table.

   For information about roles, see Environment roles in Oracle Monetization Cloud and Functional roles in Oracle Monetization Cloud .

Viewing all available roles

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To view all available roles:

1. Open the User Management application.

2. Select **Oracle Identity Self Service**.

3. Select the **Manage** button in the top right corner of the page.

4. Select **Roles**.

   The **Roles** tab appears. This tab lists all the roles in your Oracle Monetization Cloud system.

   To see details about a role, select the role's name.

   For information about roles, see Environment roles in Oracle Monetization Cloud and Functional roles in Oracle Monetization Cloud .

Removing roles from users in Oracle Monetization Cloud

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To remove a role from a user:

1. Open the User Management application.

2. Select **Oracle Identity Self Service**.

3. Select the **Manage** button in the top right corner of the page.

4. Select **Users**.

   The **Users** tab appears.

5. Use the **Search** fields to find the user whose role you want to remove.

   Users meeting the search criteria are listed in the search results.

6. In the **User Login** column, select the link of the user from which you want to remove a role.

   The **User Details** tab appears.

7. Select the **Roles** tab.

   A list of assigned roles is displayed.

8. Select the role you want to remove, and then select **Remove Roles**.
9. (Optional) Enter an effective date and a justification.
10. Select **Submit**.

Removing users from Oracle Monetization Cloud

You can remove users from Oracle Monetization Cloud in either of the following ways:

- Disabling users in Oracle Monetization Cloud: The user and all related information remain in the system. If necessary, the user can be reenabled.
- Deleting users from Oracle Monetization Cloud: The user and all related information are removed from the system. The user can't be reenabled.

Disabling users in Oracle Monetization Cloud

When you disable (inactivate) a user, the user and all related information remain in the Oracle Monetization Cloud system. If necessary, the user can be reenabled.

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To disable users:

1. Open the User Management application.
2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.
4. Select **Users**.
5. Use the **Search** fields to find the user you want to inactivate.

   Users meeting the search criteria are listed in the search results.

6. Select the row of the user to inactivate, and select **Disable**.

   The **Disable Users** tab appears.

7. (Optional) Enter an effective date and a justification.
8. Select **Submit**.

   The user is inactivated, and the user's identity status is changed to **Disabled**.

Deleting users from Oracle Monetization Cloud

When you delete a user, the user and all related information are removed from the Oracle Monetization Cloud system. The user can't be reenabled.

Only the default administrative user, *TenantSysAdmin*, can perform this task. For background information about *TenantSysAdmin*, see About Oracle Monetization Cloud users.

To delete users:

1. Open the User Management application.
2. Select **Oracle Identity Self Service**.
3. Select the **Manage** button in the top right corner of the page.
4. Select **Users**.
5. Use the **Search** fields to find the user you want to delete.

   Users meeting the search criteria are listed in the search results.
6. Select the row of the user to delete, and then select **Delete**.

   The **Delete Users** tab appears.
7. (Optional) Enter an effective date and a justification.

   > **Note:**
   >
   > Selecting **Submit** in the following step permanently removes the user from your system. To cancel this operation, close the **Delete Users** tab before selecting **Submit**.
8. Select **Submit**.

   The user is deleted.

Setting password policies for Oracle Monetization Cloud

By default, the password policy for Oracle Monetization Cloud is the following:

- Minimum length: 8 characters
- Minimum numeric characters: 1
- Minimum alphabet characters: 2
- Minimum uppercase characters: 1
- Minimum lowercase characters: 1
- Minimum special characters: 1

For information about modifying the policy, see the discussion about managing password policies in *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.

> **Note:**
>
> The default password policy provides the *minimum* level of security. If you modify it, don't weaken it.

Related topics

- About Oracle Monetization Cloud security
- About integrating your business systems

4
About data privacy

Oracle Monetization Cloud supports data privacy for all personal data by implementing data encryption, data masking, and data purging. We also encourage best practices, such as obtaining consent to collect and store personal data and implementing role-based access for applications that expose personal data.

Topics in this document

About personal data

Personal data that needs to be protected can come from your customers and your employees.

Customer personal data includes:

- **Financial information**: Credit and debit card information, bank account information, and tax exemption certificate numbers
- **Contact information**: Names, phone numbers, physical addresses, email addresses, IP addresses, preferred languages or locales, and time zones
- **Credentials**: User names, passwords, security hints, and security answers
- **Bill information**: Invoice numbers, bill amounts, bill details, and bill history

Employee personal data includes:

- Information required for setting up accounts: user names, passwords, security hints, and answers.
- Additional, optional information: employee IDs, job titles, and job descriptions.

For more information about the categories of personal data, see section 4 of *Data Processing Agreement for Oracle Cloud Services,* available on the Oracle Cloud Services contracts page:

`http://www.oracle.com/us/corporate/contracts/cloud-services/index.html`

Obtaining consent

Before collecting personal data from customers, your CSRs must obtain verbal consent to collect and store the information. You're responsible for training your CSRs to do this.

Encrypting data

Personal data is automatically encrypted as follows:

- Oracle Monetization Cloud applications encrypt password and credit card numbers.
- Connections between Oracle Monetization Cloud applications and the database are encrypted using Oracle Database Network Encryption.
- Personal data in the database is encrypted using Oracle Database Transparent Data Encryption (TDE).

Masking data in logs

Oracle Monetization Cloud automatically masks personal data in logs. This prevents users from seeing personal data if they don't need access to it to do their job, such as a system administrator troubleshooting connection issues. The users who do need to see this data, such as CSRs, can still see it in Subscriber Management.

Purging data

Oracle Monetization Cloud automatically purges old events that contain personal data after a retention period of 12 months. By default, closed accounts are also deleted 12 months after closing. This permanently deletes the account and all personal data associated with it.

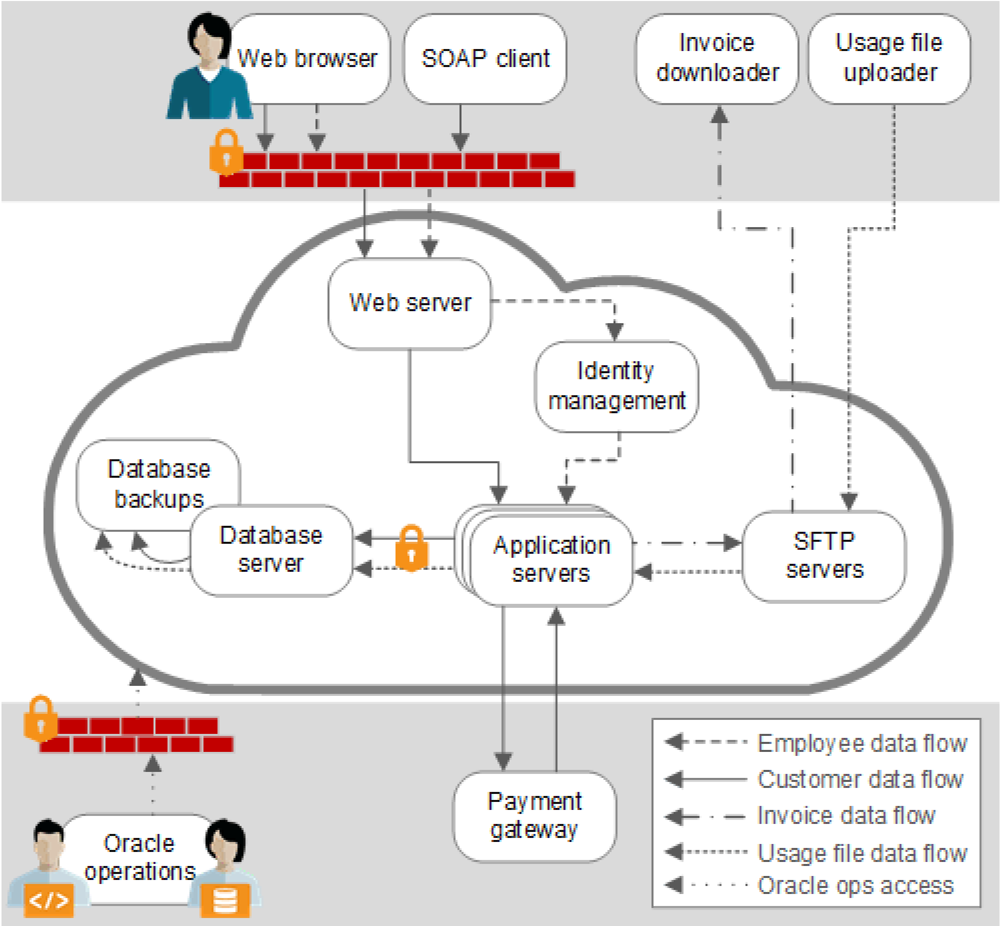
Use System Configuration to adjust the retention period for old events and closed accounts. Select **Data Privacy** and enter the number of months to retain the data. You should keep as little personal data as possible for the minimum time necessary.

> **Note:**
>
> You're responsible for purging personal data from your payment and taxation gateways and any other external systems. Oracle Monetization Cloud doesn't inform the gateways that data needs to be removed.

You can also immediately remove customer personal data on demand by using a SOAP client to call the pcmOpCustDeletePersonalData operation of the BRMCustService_v2 web service. See *Oracle Monetization Cloud Integration Guide* for information about using the SOAP web services and *Oracle Monetization Cloud SOAP API Reference* for information about this operation.

About the flow of personal data

Personal data flows securely into and out of Oracle Monetization Cloud at several points, illustrated by this graphic and described below.



Customer data flow

1. After getting consent from the customer, your CSR records personal data while creating the account and subscribing the customer to services.

   Alternatively, your customer could enter their information into your customer portal, which you have configured to call the Oracle Monetization Cloud SOAP API.

2. From the web browser or the SOAP API call, the personal data passes through the Oracle firewall and load balancers into the Oracle Monetization Cloud web server.
3. The web server sends the data to the appropriate application servers
4. The application server sends subscriber registration and payment processing data out of Oracle Monetization Cloud to the payment gateway using a REST API.
5. The payment gateway validates the subscribers and returns tokenized credit and debit card numbers to the Oracle Monetization Cloud application server.

6. The application server passes the personal data and tokens through Network Encryption to the database server.
7. The database server stores the data securely using TDE.
8. The encrypted data is backed up periodically in case you need to restore a corrupt database.
9. Only users with the appropriate authorization can access the personal data from the database.

Employee data flow

1. Using a web browser, your system administrator logs in to Oracle Monetization Cloud with the credentials that allow access to User Management.
2. The system administrator creates and manages users for the people in your organization, creating user names and passwords for them and entering any optional personal data, such as employee numbers or job titles.
3. The personal data and credentials pass through the Oracle firewall and load balancers into the Oracle Monetization Cloud web server.
4. The web server sends the data to the Oracle Identity Management server to set up user authentication.
5. Using a web browser, your employees sign in to Oracle Monetization Cloud using their new credentials.
6. The credentials pass through the Oracle firewall and load balancers into the Oracle Monetization Cloud web server.
7. The web server sends the credentials to the Identity Management server for authentication.
8. After authentication, the identity management server sends the employee to the application server that their role authorizes them to use. For example, employees with a CSR role can access Subscriber Management, and employees with a BI Publisher role can access reports.

Usage data flow

Usage data flows from your system into Oracle Monetization Cloud on an SFTP server. Access to the SFTP server is controlled by user authentication and secure keys.

Usage data flows as follows:

1. Your system records customer usage data in usage files, then uploads them to Oracle Monetization Cloud using the SFTP server.
2. The SFTP server sends the usage files to the appropriate application server for processing.
3. The application server processes the usage data and updates the usage files with success or failure messages, then passes the processed usage data through Network Encryption to the database server.
4. The database server stores the data securely using TDE.
5. The encrypted data is backed up periodically in case you need to restore a corrupt database.

6. Authorized users can access the updated usage files on the SFTP server and purge them after they're no longer useful.

Invoice data flow

Invoice data is generated on the Oracle Monetization Cloud application server and stored as PDFs or XML files on the SFTP server. Your system accesses the SFTP server by providing user credentials and secure keys, then downloads the PDF invoices for distribution to your customers.

Oracle administrator access

Occasionally, an Oracle database or system administrator may need to access your cloud system to perform maintenance or upgrades. This access is controlled by strict user roles and multi-factor authentication managed through Oracle Privileged Account Manager, and secured through Oracle firewalls, bastion hosts, multi-factor authentication, and VPN clients. All Oracle employee activity in your system is logged and tracked.

Related topics

- Implementing role-based application security