Oracle Cloud

Using Oracle Data Safe

E92975-88
June 2025

Oracle Cloud Using Oracle Data Safe,

E92975-88

Contents

4 Activity Auditing

5 Alerts

7 Data Masking

8 SQL Firewall

9 Events

10 Reference

Preface

The *Using Oracle Data Safe* guide describes how to utilize Oracle Data Safe for discovering and masking sensitive data to ensure its safety for development and testing purposes. Additionally, the guide provides instructions on assessing the security of your database and its users, auditing user activity, and generating audit reports.

Audience

The *Using Oracle Data Safe* guide is intended for those who want to use Oracle Data Safe features, including User Assessment, Security Assessment, Activity Auditing, Data Discovery, and Data Masking.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `https://www.oracle.com/corporate/accessibility/`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` if you are hearing impaired.

Related Resources

For more information, see these Oracle resources:

- Administering Oracle Data Safe
- What's New for Oracle Data Safe
- Oracle Public Cloud

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Get Started with Oracle Data Safe

Oracle Data Safe is a fully-integrated, regional Cloud service focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle databases.

Oracle Data Safe Overview

Oracle Data Safe is a unified control center for your Oracle databases which helps you understand the sensitivity of your data, evaluate risks to your data, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and address data security compliance requirements.

Features of Oracle Data Safe

Oracle Data Safe provides the following set of features for protecting sensitive and regulated data in Oracle databases, all in a single, easy-to-use database security control center:

- **Security Assessment** helps in evaluating the security of your database configurations. It examines database configurations, user accounts, and security controls, and subsequently provides findings along with recommendations for remedial actions following best practices to reduce or mitigate risks. Recommendations are based on the Security Technical Implementation Guides (STIG), Center for Internet Security (CIS) Configurations, recommendations from the General Data Protection Regulation (EU GDPR) and Oracle best practices.
- **User Assessment** assists in identifying highly privileged accounts that may pose a threat if misused or compromised. It scrutinizes information about users in the data dictionary of target databases and calculates a potential risk score for each user. This evaluation includes user types, authentication methods, password policies, password change frequency, and provides direct links to related audit records. With this information, appropriate security controls and policies can be deployed.
- **Data Discovery** facilitates the detection of sensitive data within your databases. By specifying the type of sensitive data to search for, Data Discovery examines the actual data and data dictionary, presenting a list of sensitive columns. It comes with default search capabilities covering various sensitive data categories, such as identification, biographic, IT, financial, healthcare, employment, and academic information.
- **Data Masking** offers a means to mask sensitive data, ensuring its safety for non-production purposes. For instance, when organizations need to create copies of production data for development and testing, Data Masking replaces sensitive data with realistic but fictitious information, mitigating the risk associated with exposing sensitive data to new users.
- **Activity Auditing** lets you audit user activity on your databases so you can monitor database usage.
- **Alerts** keep you informed of unusual database activities as they happen.
- **SQL Firewall** protects against risks such as SQL injection attacks or compromised accounts. SQL Firewall is a new security capability built into the Oracle Database 23ai

kernel and offers protection against these risks. The SQL Firewall feature in Oracle Data Safe lets you centrally manage and monitor the SQL Firewall policies for your target databases. Oracle Data Safe lets you collect authorized SQL activities of a database user, generate and enable the policy with allowlists of approved SQL statements and database connection paths, and provides a comprehensive view of any SQL Firewall violations across the fleet of your target databases.

Oracle Data Safe Guided Tour

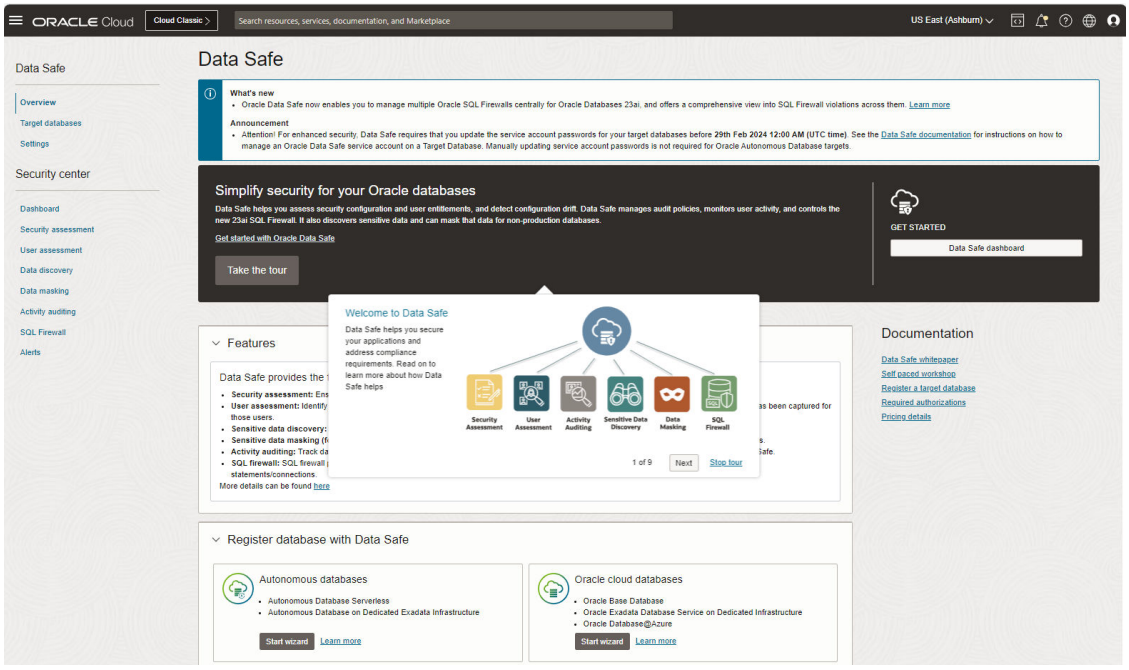
The Oracle Data Safe guided tour gives you a high-level overview of the features of Oracle Data Safe and how to start using them to improve the security of your databases.

If you do not have any target databases registered with Oracle Data Safe the tour will begin automatically. If you navigate to the Overview page again during the same session the tour will no longer start automatically.

Anyone can initiate the tour at any time by navigating to the Overview page and clicking **Take the tour**.

You can click through the walk through by clicking **Next** or stop the tour at any time by clicking **Stop tour**.

Figure 1-1 Data Safe Overview



Key Concepts and Terminology

Understand the following concepts and terminology to help you get started with Oracle Data Safe.

Oracle Cloud Infrastructure

Oracle Cloud Infrastructure is a set of complementary cloud services that enables you to build and run a wide range of applications and services in a highly available hosted environment.

Oracle Cloud Infrastructure offers high-performance compute capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network. Oracle Data Safe is integrated as a service into Oracle Cloud Infrastructure.

Oracle Cloud Infrastructure Console

The Oracle Cloud Infrastructure Console is a simple and intuitive web-based user interface that you can use to access and manage Oracle Cloud Infrastructure. You can access Oracle Data Safe in the Oracle Cloud Infrastructure Console.

Tenancy

A tenancy is a secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud resources.

Region and Availability Domain

Oracle Cloud Infrastructure is *physically* hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance.

Oracle Data Safe

Oracle Data Safe is a fully-integrated Cloud service in Oracle Cloud Infrastructure focused on the security of your data. It provides a complete and integrated set of features for protecting sensitive and regulated data in Oracle databases. The Security Center in Oracle Data Safe is the main area where you can access all the features.

Oracle Cloud Infrastructure Identity and Access Management (IAM)

The IAM service is the default, fully integrated, identity management service for Oracle Cloud Infrastructure. It lets you control who has access to your cloud resources, what type of access user groups have, and to which specific resources user groups have access. Oracle Data Safe uses all the shared services in Oracle Cloud Infrastructure, including IAM.

IAM Compartment

In IAM, compartments allow you to organize and control access to your cloud resources. A compartment is a collection of related resources, such as database instances, virtual cloud networks, and block volumes. A compartment should be thought of as a logical group and not a physical container. When you begin working with resources in the Oracle Cloud Infrastructure Console, the compartment acts as a filter for what you are viewing. A group requires permission by an administrator to access a compartment.

IAM User Group

A user group in IAM is a collection of users who all need the same type of access to a particular set of resources or compartment. Tenancy administrators can create users and groups in the root compartment of a tenancy with the IAM service in Oracle Cloud Infrastructure. Oracle Data Safe retrieves user groups from IAM, and in some cases, individual users.

Oracle automatically creates a tenancy administrator for you and adds it to the tenancy's `Administrators` group. This group has all permissions on all resources in the tenancy, and is responsible for creating the users, groups, and compartments for the tenancy.

IAM Policy

An IAM policy is a document that specifies who can access which resources in Oracle Cloud Infrastructure, and how. Access is granted at the group and compartment level, which means you can write a policy that gives a group a specific type of access within a specific compartment, or to the tenancy itself. If you give a group access to your tenancy, the group automatically gets the same type of access to all the compartments inside your tenancy. Only tenancy administrators can create policies. An administrator can create IAM policies to define user privileges for all Oracle Data Safe resources.

Oracle Data Safe Console

The Oracle Data Safe Console is the former user interface for Oracle Data Safe. Administrators need to migrate content from this Console to the new Security Center in Oracle Cloud Infrastructure.

Oracle Data Safe Repository

The Oracle Data Safe repository is an Oracle database that stores audit data and metadata for Oracle Data Safe.

Target Database

A target database is an Oracle Database on which Oracle Data Safe can perform user and security assessment, data discovery, data masking, activity auditing, and alerts.

Sensitive Type

A sensitive type is a classification of sensitive data and defines the kind of sensitive columns to search for. For example, the US Social Security Number (SSN) sensitive type helps you discover columns containing Social Security numbers. Data Discovery searches for sensitive data in your databases based on the sensitive types that you choose. You can choose from a wide variety of predefined sensitive types and can also create your own sensitive types.

Sensitive types are divided into categories. The top-level categories are Identification Information, Biographic Information, IT Information, Financial Information, Healthcare Information, Employment Information, and Academic Information. You can choose individual sensitive types or sensitive categories to search sensitive data.

Sensitive Data Model

A sensitive data model is a collection of sensitive columns and referential relationships. Data Discovery identifies sensitive columns and referential relationships and creates a sensitive data model. Data Discovery automatically searches the Oracle data dictionary to find relationships between primary key columns and foreign key columns and flags them as sensitive. It can also discover non-dictionary referential relationships, which are relationships defined in applications and not in the Oracle data dictionary.

Masking Format

A masking format defines the logic to mask sensitive data in a database column. For example, the Shuffle masking format randomly shuffles values in a column. The Email Address masking format replaces values in a column with random email addresses. Oracle Data Safe provides many predefined masking formats. If needed, you can create your own.

Masking Policy

A masking policy maps sensitive columns to masking formats that should be used to mask the data. You can use a masking policy to perform data masking on a target database. You can create a masking policy using a sensitive data model.

Audit Data Retrieval

An audit data retrieval represents an archive retrieve request for audit data. You can retrieve audit data for a target database from the archive and store it online.

Audit Policy

An audit policy represents the audit policies for the target database and their provisioning status on the target database.

Audit Profile

An audit profile represents audit profile settings and audit configurations for the database target, and helps determine the audit data volume available on the target and the volume collected by Oracle Data Safe.

Alert Policy

In Oracle Data Safe, you can provision alert policies on your target databases. An alert policy defines an event in a database to monitor. Alert policies are rule-based and are triggered based on the audit data collected.

Audit Trail

An audit trail represents the source of audit records that provides documentary evidence of the sequence of activities in the target database.

Alert

An alert is a message that notifies you when a particular audit event happens on a target database.

Try Oracle Data Safe for Free

Oracle offers a free tenancy and a 30-day free trial for a variety of Oracle Cloud Infrastructure services, including Oracle Data Safe. You can sign up for a free Oracle cloud account, and then try Oracle Data Safe with your Oracle cloud or on-premises Oracle databases.

Overview

During a free trial, you can try out all of the main features of Oracle Data Safe in your tenancy, including Activity Auditing, User Assessment, Security Assessment, Data Discovery, and Data Masking. For more information, see Trial Period.

When the free trial period ends, you have a 30-day grace period in which you can still use existing resources in Oracle Data Safe. For example, you can continue to use the databases that you registered with Oracle Data Safe during your free trial. For more information, see Grace Period.

When the grace period ends, you no longer have access to Oracle Data Safe, your target databases are deregistered from Oracle Data Safe, and all Oracle Data Safe resources are reclaimed by Oracle. At any time, you can convert your free Oracle cloud account to a paid account. With a paid account, you can use all of the features of Oracle Data Safe, and opt for paid usage for audit collection. You can also register an unlimited number of target databases. Be aware that you are billed when you register an on-premises Oracle Database or an Oracle Database on a compute instance.

Trial Period

For the first 30 days, you can do the following with Oracle Data Safe:

- Register one or more of the following paid or free Cloud databases in your tenancy with Oracle Data Safe:
  - Oracle Autonomous Database Serverless (Secure access from everywhere, Secure access from allowed IPs and VCNs only, or Private endpoint access only)
  - DB system (Virtual Machine, Bare Metal, or Exadata)
- Register up to one paid on-premises Oracle Database or one paid Oracle Database on a compute instance. During the free trial period, billing for registering these two types of databases is waived.
- Create up to two Oracle Data Safe private endpoints per region in your tenancy.
- Create one Oracle Data Safe on-premises connector per region in your tenancy.
- Use all Oracle Data Safe features with your registered target databases. You can configure audit trail collection for up to one million audit records per target database per month. Audit collection is automatically stopped after you reach the limit. Only non-paid audit collection is allowed. You cannot configure or change the audit data retention period. If you later convert your tenancy to a full-use tenancy, you can retroactively apply longer-term retention policies to the audit data you collected during the trial period. Auto-purge is disabled, meaning Oracle Data Safe will not delete any audit records on your target database.

Grace Period

When the 30-day trial period ends, you have another 30-days of grace period during which you can continue to use the following:

- Existing Oracle Data Safe services that you enabled during the trial period.
- Existing registered target databases. You cannot register any new target databases.
- Existing Oracle Data Safe private endpoints and/or an existing Oracle Data Safe on-premises connector for already registered target databases. You cannot create and deploy a new private endpoint or on-premises connector.
- All Oracle Data Safe features supported for the target databases that you registered during the trial period. You can continue to collect up to one million audit records per target database per month. Audit collection is automatically stopped after you reach the limit. Only non-paid audit collection is allowed. Auto-purge is disabled, meaning Oracle Data Safe will not delete any audit records on your target database.

Set Up Oracle Data Safe

To use Oracle Data Safe features with your databases, you need to set up an Oracle Data Safe environment. Setup involves registering target databases.

Please refer to the following information in the *Administer Oracle Data Safe* guide:

- Target Database Registration

Access Oracle Data Safe

You can access Oracle Data Safe through the navigation menu in the Oracle Cloud Infrastructure Console.

1. To sign in to an OC1 realm (for most commercial and user accounts), open a supported browser and enter the following URL:

   ```
   https://cloud.oracle.com
   ```

   To sign in to a different realm, include the realm in the URL; for example `https://oc2.cloud.oracle.com`, where `oc2` is the realm name.

   If you directly access and sign in to the Oracle Data Safe Console via a previously saved bookmark, then when you navigate to an Oracle Cloud Infrastructure native feature (for example, Security Assessment), you are presented with an Oracle Cloud Infrastructure login page. Click **Next** to continue to the feature. You do not need to reenter your user credentials.
2. In the **Cloud Account Name** field, enter your tenancy name, and then click **Next**.

   The **SIGN IN** page is displayed.
3. If the **Single Sign-On** option is presented on your sign-in page, it means that your tenancy is federated with an identity service other than the default one. You can sign in the following way:
   a. Select your identity provider and click **Continue**.

      You are redirected to your identity provider to sign in.
   b. Enter your user name and password.

   You are signed in to your home region in the Oracle Cloud Infrastructure Console.
4. If the **Single Sign-On** option is not presented on your sign-in page, then your tenancy uses the default identity service, which is Oracle Cloud Infrastructure Identity and Access Management (IAM). You can sign in the following way:
   a. Enter your Oracle Cloud Infrastructure user name and password, and then click **Sign In**.
   b. If you are signing in for the first time, you are prompted to change your temporary password. Enter a new password, making sure to follow the password criteria, and click **Submit**.

   You are signed in to your home region in the Oracle Cloud Infrastructure Console.
5. (Optional) In the upper-right corner of the window, select the appropriate region in your tenancy; for example, **US East (Ashburn)**.

Oracle Data Safe resources, such as sensitive data models, masking policies, and registered target databases are region-specific. Therefore, you want to make sure that you select Oracle Data Safe in the region that contains the resources that you need.

6. From the navigation menu, select **Oracle Database**, and then **Data Safe - Database Security**.

   The **Overview** page for the Oracle Data Safe service is displayed.

Oracle Data Safe Dashboard

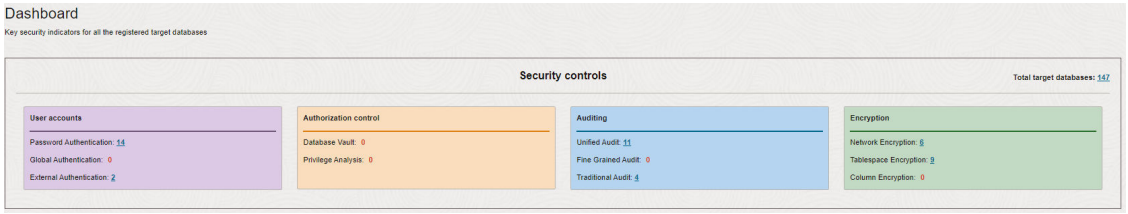
When you sign in to Oracle Data Safe, you are presented with a dashboard, which consists of several charts that you let you monitor activities.

The dashboard has a **Security controls** section and a **Feature metrics** section.

The **Security controls** section provides a fleet-wide view of the security measures used across your target databases in the selected compartment. Oracle databases have several security measures built into the database and this section shows you how many of your target databases have certain security measures enabled. Analyzing this information provides you with insight into the potential security threats that your target databases are exposed to based on the security messures that are or are not enabled.

Click on the numbers next to each security measure to see a more detailed view of which target databases have the listed security measures enabled. Click on the name of any target database to view the latest security assessment for the selected database.

The following screenshot is an example of the **Security controls** section.



The **Feature metrics** section has the following charts:

- **Security Assessment:** View the percentage of advisory, evaluate, low, medium, and high risk security configurations in your databases.
- **User Assessment:** View the percentage of low, medium, high, and critical potential risk users in your database.
- **Data Discovery:** View the top five sensitive columns in your top five target databases.
- **All Activity:** View the number of audit events per day for the past one week performed by all users.
- **Admin Activity:** View the number of audit events per day for the past one week performed by admin users.
- **Open Alerts:** View the number of open alerts per day for the past one week.
- **Feature Usage:** View the number of target databases using each Oracle Data Safe feature (Security Assessment, User Assessment, Data Discovery, Data Masking, and Activity Auditing).

- **Operations Summary:** View the number of failed, in progress, succeeded, and accepted operations for Security Assessment, User Assessment, Data Discovery, and Data Masking for the past one week.
- **Audit Trails:** View the number of audit trails that are running, stopped, in transition, needs attention, and failed.

If you are accessing Security Center for the first time, then the charts may have no data to display. After you register a target database, Oracle Data Safe automatically performs a User Assessment and Security Assessment for your target database, which populates the Security Assessment and User Assessment charts in the dashboard. You can filter the data in the dashboard by compartment and target database.

The following screenshot is an example of the **Feature metrics** section.

2

Security Assessment

This section discusses how to assess database security using the Security Assessment feature of Oracle Data Safe.

Security Assessment Overview

The Security Assessment feature in Oracle Data Safe assess the security of your Oracle databases.

About Security Assessment

Misconfigured databases are a major contributor to database breaches. Human errors could leave your database open to everyone, or an attacker could maliciously exploit configuration mistakes to gain unauthorized access to sensitive data. This can have a devastating impact on your reputation and bottom line. Knowing where your database configuration introduces risk is the first step in minimizing that risk. Security Assessment provides you with an overall picture of your database security posture. It analyzes your database configurations, user and their entitlements as well as security policies to uncover security risks and improve the security posture of Oracle databases within your organization. A security assessment provides findings with recommendations for remediation activities that follow best practices to reduce or mitigate risk. The information presented depends on the type of target database and whether it is running on-premises or in the cloud. Specific checks and recommendations are made for Autonomous Databases, Oracle Base Database Service, and on-premises Oracle Databases.

For all registered target databases, Security Assessment automatically generates an assessment once per week and saves a copy of it to the history. This report is referred to as the "latest" assessment. If needed, you can modify its schedule. You also have the option to create a schedule that saves a copy of the latest assessment to a different compartment and with a different name.

Security Assessment lets you refresh the latest assessment at any time by using the Refresh Now option. After the latest assessment is refreshed, Security Assessment saves the assessment to the history and also overwrites the latest assessment. To monitor security configuration drift on your target database, you need to set a baseline. Once your baseline is set, Data Safe automatically compares it against each assessment refresh. You can also manually compare two selected assessments. Lastly, you can generate a PDF or XLS report from an assessment.

The following are use cases for the Security Assessment feature:

- Identify and mitigate risks:
  - Quickly and easily assess your database configurations to learn which configuration choices may have introduced unnecessary risk and how you can remove, or mitigate risks.
  - Leverage checks that range from Oracle Database security best practices, CIS Benchmark recommendations, best practices from the General Data Protection Regulation (GDPR) to Department of Defense Security Technical Implementation Guide (STIG) rules.

- Compliance and best practices:
  - Support your regulatory compliance efforts by adhering to security best practices and industry standards.
  - Track remediation and compliance progress by customizing the risk level associated with a finding.
- Improve database security insight:
  - Get visibility to fleet-wide database security risks.
  - Monitor security drift by comparing an assessment against a baseline.
  - Get visibility into deployed security policies and get awareness of available database security controls to further protect your data.

Risk Levels

You can use the Risk Level values as guidelines for implementing Security Assessment recommendations. They can be used to prioritize and schedule changes based on the level of risk, and what it might mean to your organization. Security Assessment uses the following risk levels to measure the severity of a finding:

- High: Needs immediate attention.
- Medium: Plan to address this in the short term.
- Low: Might be fixed during a scheduled downtime or bundled together with other maintenance activities.
- Advisory: Improve security posture by enabling more security features and technology.
- Evaluate: Needs manual analysis.
- Pass: No risks found.
- Deferred: The user deliberately decided to postpone or delay taking action on a particular identified risk for a specified period of time or indefinitely. When a risk is deferred, it means that, after evaluation, it has been acknowledged but not immediately addressed.

Categories

Security Assessment categorizes its findings as follows:

- User Accounts
- Privileges and Roles
- Authorization Control
- Fine-Grained Access Control
- Auditing
- Encryption
- Database Configuration

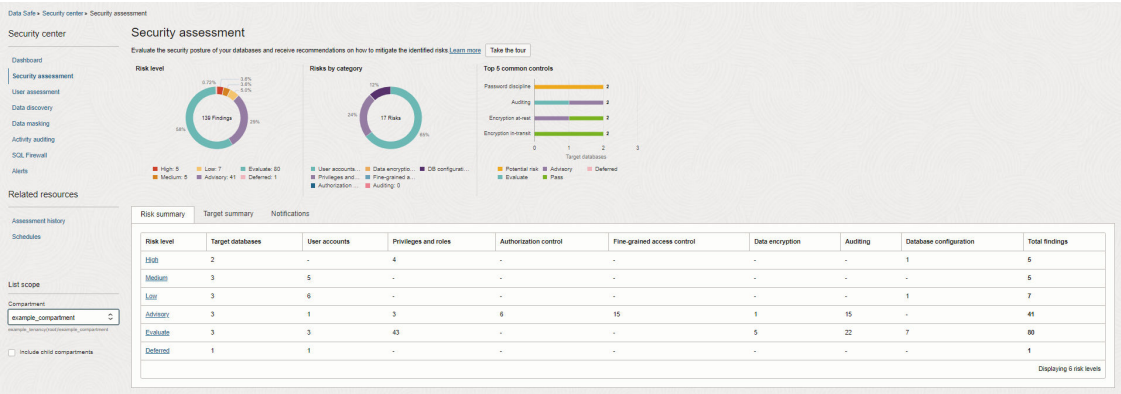
Security Assessment Dashboard

When you first access the main page for Security Assessment in the Data Safe Security Center, you are presented with a dashboard that consists of these components:

- **Risk level**, **Risks by category**, and **Top 5 common controls** charts
- **Risk summary** tab
- **Target summary** tab
- **Notifications** tab
- **Related resources**
- **List scope**

You can explore key features and workflows with the guided tour option by clicking the "Take the tour" button in the Security Assessment dashboard.

> **Note:**
>
> You can view assessments only within compartments where you have the required privileges.



Charts

At the top of the **Security Assessment** page, you can view the **Risk Level**, **Risks by Category**, and **Top 5 common controls** charts.

The **Risk level** chart shows you a percentage breakdown of the different risk levels (High, Medium, Low, Advisory, Evaluate, and Deferred) across all of your target databases.

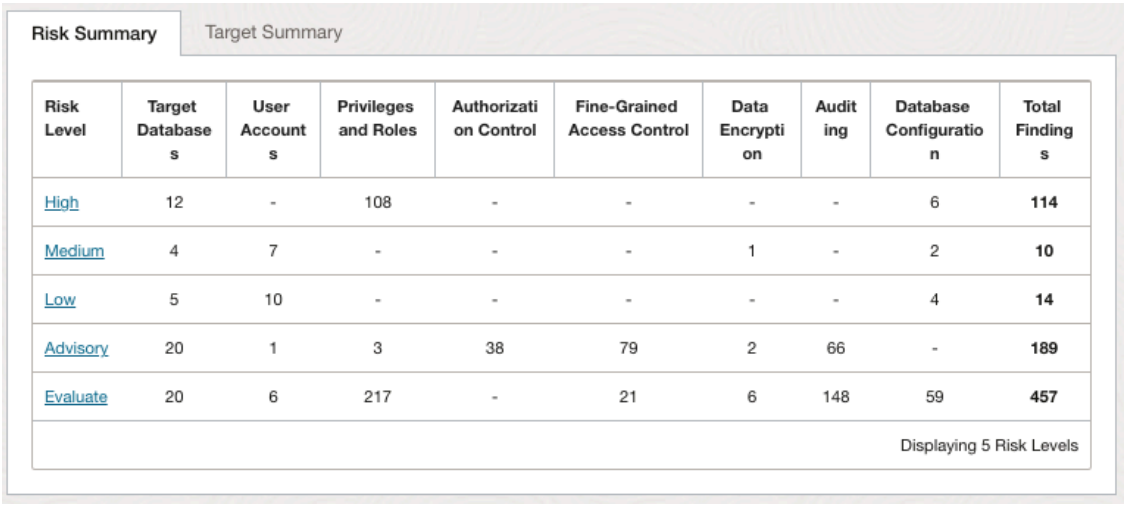
The **Risks by category** chart shows you a percentage breakdown of the findings in each risk category (User Accounts, Privileges and Roles, Authorization Control, Data Encryption, Fine-Grained Access Control, Auditing, and Database Configurations) across all of your target databases.

The **Top 5 common controls** chart shows a bar graph of the number of target databases at each risk level for each of the top five common controls. The top five common controls are the five security controls that Oracle considers the most important to the security of your target databases. Clicking on any of the bars will show you the list of target databases associated with the selected data.

> **Note:**
>
> The **Potential risk** category in the **Top 5 common controls** chart includes any high, medium, and low risk findings.

Risk Summary

The **Risk Summary** tab lets you quickly view the number of risk findings per risk level across all of your target databases in a selected compartment. There is one table row for each risk level: High, Medium, Low, Advisory, Evaluate, and Deferred. For each risk level, you can view the number of findings for the following categories: User Accounts, Privileges and Roles, Authorization Control, Fine-Grained Access Control, Data Encryption, Auditing, and Database Configuration. From this page, you can drill down to view more information about the identified risks, and then drill down further to view information about a particular target database.



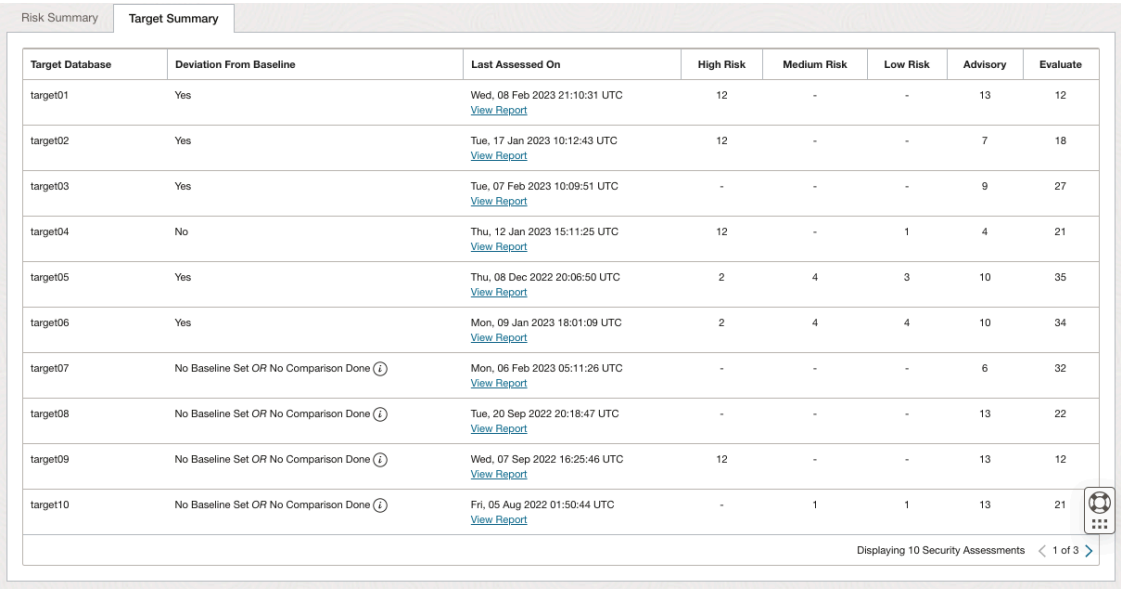
Risk Summary | Target Summary

Risk Level	Target Databases	User Accounts	Privileges and Roles	Authorization Control	Fine-Grained Access Control	Data Encryption	Auditing	Database Configuration	Total Findings
High	12	-	108	-	-	-	-	6	**114**
Medium	4	7	-	-	-	1	-	2	**10**
Low	5	10	-	-	-	-	-	4	**14**
Advisory	20	1	3	38	79	2	66	-	**189**
Evaluate	20	6	217	-	21	6	148	59	**457**

Displaying 5 Risk Levels

Target Summary

The **Target Summary** tab shows you the number of findings for each risk level (High, Medium, Low, Advisory, Evaluate, and Deferred) per target database, the date of the last assessment, and whether the latest assessment deviates from the baseline (assuming you set a baseline). You can also access a link to the latest Security Assessment report for each target database. If an assessment failed, a FAILED icon (yellow yield sign with an exclamation mark) is displayed in the **Last Assessed On** column for the target database.



Notifications

The **Notifications** tab shows you what event notifications and subscriptions you have created for Security Assessment. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show events that you have created directly within Data Safe. If you haven't created any event notifications for Security Assessment in Data Safe yet, you will see the list of quick start templates allowing you to create a notification for the most common events. In addition to displaying existing event notifications, you can also create new notifications by using the **Create notification** button. See Create and Modify Event Notifications in Security Assessment for more information.

Related Resources

The **Related Resources** list varies, depending on what is most useful in relation to the page you are currently looking at. At the level of the dashboard, it includes links to the **Assessment reports**, **Assessment history**, **Assessment templates**, and **Schedules** pages. If you are looking at a particular assessment it provides options to compare that assessment with other assessments.

List Scope

List Scope is where you set the scope of the lists in the **Risk Summary** and **Target Summary** tabs. It determines which compartments are included in those lists.

You can set the scope of your view of Security Assessment to the root compartment alone or root with all of its child compartments or to any compartment under root with or without that compartment's child compartments.

Setting the scope to root with its child compartments allows you to review the overall security posture of your tenancy, or you can focus on a specific compartment by narrowing the scope to that compartment.

> **Note:**
>
> It's important to remember that within the selected scope, your view within Security Assessment is determined by the privileges your account has been granted in OCI.

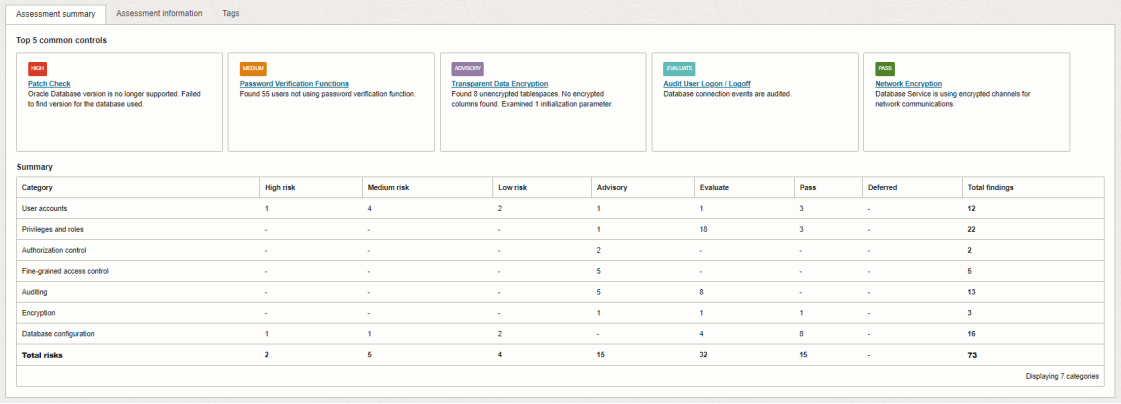
Structure of a Security Assessment

A Security Assessment for a target database consists of the following five sections:

- **Assessment Summary** tab
- **Assessment Information** tab
- **Tags** tab
- **Assessment Details** section
- **Resource and Filters** section

Assessment Summary Tab

This tab shows you at a glance the security posture of your target database. This tab presents the risk level of the **Top 5 common controls** and the number of findings per category per risk level. The **Top 5 common controls** are the five security controls that Oracle considers the most important to the security of your target databases. Clicking on any of the top 5 common controls will direct you to the specific finding in the Assessment Details, where you can find more information.

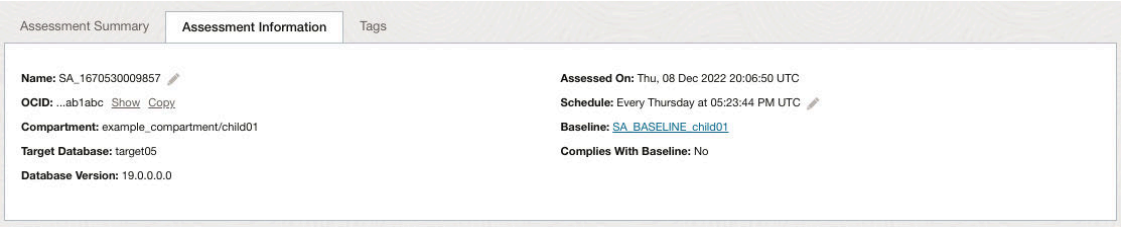


Assessment Information Tab

This tab shows you the following metadata for the report:

- Name and OCID of the assessment.
- Compartment in which the assessment is stored, the target database name and version
- Assessment date and time
- The schedule of the assessment (you can change this schedule as needed)

- Baseline (if set)
- Complies with Baseline (**Yes**, **No**, or **No Baseline Set**). This field is populated depending on if a baseline was previously set and you compared this assessment with the baseline.



> **Tip:**
>
> On the Assessment Information tab you can change the auto-generated name of the assessment to a name that has specific meaning for your organization. You and other users can then more easily identify assessments. For example, you could change the name of the autogenerated security assessment `SA_1670530009857` to `SA_target05`.

Tags Tab

This tab lets you manage Oracle Cloud Infrastructure tags for the Security Assessment.

Security Assessment Workflow

This is an example workflow for Security Assessment.

1. Register your target databases in Oracle Data Safe and obtain the necessary permissions in IAM.
   When registration of a target database is complete, a security assessment of the target database runs automatically and is scheduled to run again each week at the same day and time as the registration day and time. This is the default schedule. Every time the job is executed, the new results are designated the latest assessment for the target database and a copy is saved to the history.
2. On the Security Assessment Dashboard, view and analyze the risks across all target databases in compartments where you have access rights. This gives you a broad view of your overall security posture.
3. On the dashboard, check for the highest level risks and then drill down to the latest assessements for the target databases where these risks occur. The details about these risk are explained in each assessment.
4. Analyze the risk details, take appropriate actions to mitigate risk levels in a target database, and adjust risk levels based on your analysis or requirements. You might need to adjust certain risk levels to match your policies or reflect that other security controls are in place, or choose to defer that risk.
5. Once you have taken the appropriate actions to address the identified risks in a target database, refresh the assessment and check the findings again to see if the risk levels have lowered as expected. If so, you may want to consider setting this assessment as the baseline (see step 8 for more information).
6. If required, Adjust the schedules of your security assessments to suit the needs of your organization.

7. Change the names of your security assessments to names that are meaningful to you. The default names that Oracle Data Safe assigns follow this pattern: `SA_<unique number>`. It's helpful to choose your own names. You may want to retain the `SA_` prefix because it will distinguish security assessments from user assessments (`UA_`).
8. If the risk findings in security assessment of a target database are low and you are confident that it represents a reasonably solid security posture, consider setting that assessment as the baseline for that target database. This is optional, but highly recommended because it gives you the means to compare future assessments against a known good assessment.
9. When you have accumulated two or more security assessments of a target, run a comparison of the latest assessment with earlier assessments (or with the baseline) to determine if there is any security drift.
10. Create a downloadable PDF or XLS versions of the your security assessments.
11. Save a copy or schedule saves of a copy of the latest assessment for a target database. All assessments are saved in the history provided by Security Assessment, but the Save As option can be useful if you want an additional backup or want to export the assessment findings to another compartment.
12. Set up event notifications. For example, you can subscribe to the `SecurityAssessmentDriftFromBaseline` event to be automatically informed if a security assessment differs from the baseline.

Prerequisites for Using Security Assessment

Security Assessment requires registered, properly provisioned target databases. Users must be granted specific permissions in IAM.

These are the prerequisites for using Security Assessment:

- **Register the target databases that you want to assess with Security Assessment.** After you register the target database, Oracle Data Safe automatically runs a Security Assessment job for your target database and updates it according to the schedule (once per week by default).
- **Grant the `ASSESSMENT` role to the Oracle Data Safe service account on the target database (non-Autonomous databases only).**
  An Autonomous Database is automatically provisioned with the equivalent `DS$ASSESSMENT_ROLE` when it is registered as a target database; therefore, you do not need to grant a role.
- **Obtain permission in Oracle Cloud Infrastructure Identity and Access Management (IAM).**
  Obtain either the `view` or `manage` permission for the `security-assessments` resource in IAM in the relevant compartments.

  An OCI administrator can grant these permissions.
- **Obtain `read` permission on the `data-safe-work-requests` resource in IAM if you need to set baselines or compare assessments.**

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-assessment-family` in the relevant compartments, which would include permissions on all of the resources above as well as `user-assessments`. See data-safe-assessments-family Resource in the *Administering Oracle Data Safe* guide for more information.

See Also:

The *Administering Oracle Data Safe* guide provides these sections to help with establishing the prerequisites:

- Grant Roles to the Oracle Data Safe Service Account on Your Target Database describes the roles required for Security Assessment and for other Oracle Data Safe features.
- security-assessments Resource provides the policy statement for granting users read permissions on `security-assessments`.
- data-safe-work-requests Resource provides the policy statement for granting users read permissions on `data-safe-work-requests`.

Recommended Before You Start

Oracle recommends you try the *Get Started with Oracle Data Safe Fundamentals* workshop in LiveLabs before you use Security Assessment.

The *Get Started with Oracle Data Safe Fundamentals* workshop includes hands-on training for Security Assessment. Whether or not you've taken the workshop before, you'll find that the lab for Security Assessment provides an up-front familiarity with this feature that makes it easier for you to put it to work in your organization. Consider going through the workshop to learn about Security Assessment before you proceed.

Try it now:

Get Started with Oracle Data Safe Fundamentals

Analyze Security Risk

The Security Assessment dashboard provides several views about the security risks across all of your target databases.

The **Risk Summary** shows you how much risk you have across all of your target databases. You can compare the number of high, medium, low, advisory, evaluate, and deferred risk findings across all of your target databases, and view which risk categories have the greatest numbers. From this tab, you can drill down into a risk level to view details about the risks. If you are reviewing a risk and are interested in a particular target database, you can drill down further into it to view how it is contributing to the risks.

The **Target Summary** shows you a view of the security posture of each of your target databases. You can view the number of high, medium, low, advisory, evaluate, and deferred risks for each database. You can also see, at a glance, if the latest assessment deviates from the baseline and the assessment date. This view also provides a link to the latest assessment for each target database.

Analyze Security Risk for a Target Database

You can access the latest assessment report to analyze the security risk for a target database by going through the Target Summary tab.

Steps

1. From the **Security Assessment** page, click the **Target Summary** tab.
2. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the row in the table for your target database, and click **View Report**.

   The **Security Assessment Details** page is displayed, showing you the latest assessment report for your target database. At the top of the report, the **Assessment Summary** tab is displayed by default.
5. On the **Assessment Summary** tab, view the information in the table to see at a glance how secure your database is. The **Top 5 common controls** are the five security controls that Oracle considers the most important to the security of your target databases. You can see what risk level your target database was assessed at for each of these controls. Click on any of these controls to see the **Assessment Details**. The Summary table shows you the number of findings per category per risk level.
6. Click the **Security Assessment Information** tab to view metadata about the report.
7. To specify OCI tags for the assessment, click the **Tags** tab and add tags.
8. In the **Assessment Details** section at the bottom of the page, expand the categories to view all of the information about the risk findings.
9. (Optional) Under **Filters** on the left, you can filter by risk level or data compliance reference.
   - To filter by **Risk Level**, click the check boxes for each risk level (High, Medium, Low, Advisory, Evaluate, Deferred, and Pass) to filter the information displayed in the **Assessment Details** section. Alternatively, you can select the **ALL** check box to show all risk levels.
   - To filter by **Reference**, click the check boxes for each reference (**DISA STIG**, **CIS Benchmark**, **EU GDPR**, and **Oracle Best Practices**) to filter the information displayed in the **Assessment Details** section. Alternatively, you can select the **ALL** check box to show all reference types.

> **See Also:**
>
> For more information about Assessment Details, see Security Assessment Overview.

Analyze Security Risk For All Target Databases

By analyzing the security risk across all your target databases you can identify risks and recommendations across your database fleet.

Steps

1. From the Data Safe home page in Oracle Cloud Infrastructure, under **Security Center** on the left, click **Security Assessment**.
2. Select the compartment that contains the target database(s) for which you want to aggregate the findings.
   - (Optional) Deselect **INCLUDE CHILD COMPARTMENTS** to not include findings for target databases that reside in all of the child compartments.
   - To view all findings available to you in the tenancy/region, select the **root** compartment and leave **INCLUDE CHILD COMPARTMENTS** selected. This presents the findings from all compartments that you have the privileges to access.
3. Analyze how much risk you have across all of your target databases:
   a. View the **Risk level**, **Risks by category**, **Top 5 common controls** charts.
   b. On the **Risk Summary** tab, examine the number of findings discovered across the target databases and for each risk category.
   c. To view more details about the risks, including explanations and recommendations, click a risk level link in the **Risk Level** column. The **Risk Details** page is displayed. It consists of a **Risks by category** chart and a **Risk Details** section. The **Risk Details** section shows the risks and how many target databases have this risk. Expand the risks in each category to view remarks and affected target databases. The remarks explain the risk and recommend actions for remediation.
   d. To view details for a particular target database, click the target database link in the risk. Details about the risk finding for the target database are displayed.
   e. Click **Close**.

> **Note:**
>
> When you look at risk findings and target database in Security Assessment, you can set the scope to root with its child compartments to review the overall security posture of your tenancy. You can also set the scope to focus on a specific compartment of interest.
>
> It's important to remember that within the selected scope, your view within Security Assessment is determined by the privileges your account has been granted in OCI.

Adjust the Risk Level of a Risk Finding

Once you have taken appropriate actions to mitigate security risks on a target database based on the results of a security assessment, you can adjust the risk level of a finding. Adjustments of risk levels can be indefinite or have an expiration date. Upon expiry, the next assessment resumes evaluating the finding and displays as found.

Following the initial identification of risks, the next step usually involves validating the identified risk levels before taking remediation actions. Occasionally, the identified risk is not applicable as there might be some other mitigating control in place, or it might not be necessary to fulfill your business or auditor requirements. If this is the case, you might want to have Data Safe adjust the reported findings to match your organization's specific needs. Having the ability to change the risk level will also help you to streamline and govern the assessment process.

Based on your circumstances it may be appropriate to adjust the risk level of a risk finding. You can set the risk level of a finding to be any of the risk levels automatically generated by Oracle (high, medium, low, evaluate, or pass), or can you set the risk level to deferred. A risk level of deferred allows you to indicate that after evaluation, it has been acknowledged but not immediately addressed. You are delaying taking action on a particular identified risk for a specified period of time or indefinitely so that it doesn't show up again as a risk in subsequent reports.

For example, if a risk finding has been designated by Oracle at the evaluate risk level, you should first read the details provided in the Security Assessment. Once you have read the details you may decide that there is no security risk to your target database and set the risk level to pass. When the security assessment is next refreshed, either manually or based on its schedule, the risk level will remain pass.

Alternatively, you may be in a situation in which your organization is planning to make adjustments to its password requirements in a few months. However, the current security assessment is designating "Case-Sensitive Passwords" as a high risk level. You may wish to adjust the risk level of this finding to deferred until your organization has implemented the new password requirements. You can do this by specifying an expiration date for the adjusted risk level. Upon expiry, the next security assessment for that target will resume evaluating the finding. At that time, the risk identified on the target database will start displaying as it is found in the target database.

To adjust the risk level of a risk finding:

1. Under **Security center**, click **Security assessment**.
2. From the **Security Assessment** page, click the **Target Summary** tab.
3. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

   > **Note:**
   >
   > The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The Security Assessment Details page is displayed, showing you the latest assessment report for your target database.
6. In the **Assessment details** section, click on the pencil icon for the risk finding that you would like to adjust.
7. Select either **Defer risk** or **Change risk**.
8. If you're changing the risk, select the new risk level.

9. Optionally, provide a justification for adjusting the risk.
10. Optionally, provide an expiration date for the risk adjustment.
11. Click **Save**.
    Once the risk level finishes updating you will see an indicator that the risk level for this finding has been modified.

Related Topics

- View the Risk Modification Report

Assessment Reports

Assessment Reports provide a structured view of security assessment findings. There are two reports to choose from: one report with aggregated risks across your fleet and one with target database-specific details for each risk finding. You can customize the reports, generate download reports, and save them for future use. This provides better visibility into risks across your environment and streamlines compliance reporting.

About Security Assessment Reports

Assessment Reports provide detailed insights into security assessment findings across your databases or fleet. These reports help you analyze security risks, compliance gaps, and database vulnerabilities based on predefined or customized criteria.

The **Security Assessment Reports** page includes two tabs:

- **Predefined Reports:** Provides a list of standard reports that summarize security risks based on standardized formats.
- **Custom Reports:** Provides a list of all predefined reports that have been customized and saved, but cannot be modified further.

Predefined Reports
Predefined reports offer comprehensive visibility into all security risks identified through security assessments across all database targets. The following reports are available:

- **All Risks (aggregated):** Summarizes how many database targets are affected by each finding across different risk levels.
- **All Risks (detailed):** Provides a comprehensive view of all findings across all database targets and risk levels.

View Security Assessment Reports

On the **Security assessment reports** page, you can view the list of available security assessment reports for all target databases within the compartments that you have selected and where you have the required privileges.

The **Predefined Reports** tab provides structured assessments of security risks across all database targets. You can view reports such as **All risks (aggregated)** and **All risks (detailed)**.

The **Custom Reports** tab lists all predefined reports that have been customized and saved.

1. Under **Security center**, click **Security assessment**.

2. Under **Related resources**, click **Assessment reports**. The **Security assessment reports** page is displayed.
3. (Optional) Narrow the scope of the reports by using **List scope**.
    a. Select a compartment you have access to from the **Compartment** list.
    b. Select or deselect **Include child compartments**. If you select the root compartment and allow the default **Include child compartments**, then child compartments where you have required privileges are included.
4. Within the **Predefined reports** tab, the table includes the **Report name** and **Description**. Additionally, you can do the following:
    - Click **All risks (aggregated)** to view a summary of how many database targets are affected by each finding across different risk levels.
    - Click **All risks (detailed)** to get a comprehensive view of all findings across all database targets and risk levels.
5. Within the **Custom reports** tab, you can see all predefined reports that have been customized and saved.

View All Risks (Aggregated)

On the **Security assessment reports** page, you can view the list of available security assessment reports for all target databases within the compartments that you have selected and where you have the required privileges. You can **Generate reports**, **Download reports**, and complete **More actions** within this page.

Within the **Overview** tab, you can view the **Risks by Targets** table. You can also apply filters to narrow the scope.

1. Under **Security center**, click **Security assessment**.
2. Under **Related resources**, click **Assessment reports**.
3. (Optional) Narrow the scope of the reports by using **List scope**.
    a. Select a compartment you have access to from the **Compartment** list.
    b. Select or deselect **Include child compartments**. If you select the root compartment and allow the default **Include child compartments**, then child compartments where you have required privileges are included.
4. View the list of available security assessment reports in the table.
   The table includes two tabs: **Oracle predefined reports** and **Custom reports**. Within the **Oracle predefined reports** tab, the table includes the **Report name** and **Description**.
5. Click **All risks (aggregated)** to view all risks for target databases in the specified compartment.
6. Within the **Overview** tab, click **+ Add Filter** to apply optional filters to limit the scope.
7. Click **Manage Columns** to manage the columns within the **Risks by Targets** table.
8. Click a specific risk to see the list of targets in a list.
9. (Optional) Click **Generate Report**. The report is generated and saved to the specified compartment. When the report is finished generating, do one of the following:
    - In the **Generate Report** dialog box, click the **click here** link. A dialog box is displayed where you can specify whether you want to open or save the file.

- Click **Close** to close the **Generate Report** dialog box, and then click **Download Report**. A dialog box is displayed where you can specify whether you want to open or save the file.

View All Risks (Detailed)

On the **Security assessment reports** page, you can view the list of available security assessment reports for all target databases within the compartments that you have selected and where you have the required privileges. You can **Generate reports**, **Download reports**, and complete **More actions** within this page.

1. Under **Security center**, click **Security assessment**.
2. Under **Related resources**, click **Assessment reports**.
3. (Optional) Narrow the scope of the reports by using **List scope**.
   a. Select a compartment you have access to from the **Compartment** list.
   b. Select or deselect **Include child compartments**. If you select the root compartment and allow the default **Include child compartments**, then child compartments where you have required privileges are included.
4. View the list of available security assessment reports in the table.
   The table includes two tabs: **Oracle predefined reports** and **Custom reports**. Within the **Oracle predefined reports** tab, the table includes the **Report name** and **Description**.
5. Click **All risks (detailed)** to view all risks for target databases in the specified compartment.
6. Within the **Overview** tab, click **+ Add Filter** to apply optional filters to limit the scope.
7. Click **Manage Columns** to manage the columns within the **Risks by Targets** table.
8. Click a specific risk to see the details of the risk in the selected target database.
9. (Optional) Click **Generate report**. The report is generated and saved to the specified compartment. When the report is finished generating, do one of the following:
   - In the **Generate Report** dialog box, click the **click here** link. A dialog box is displayed where you can specify whether you want to open or save the file.
   - Click **Close** to close the **Generate Report** dialog box, and then click **Download Report**. A dialog box is displayed where you can specify whether you want to open or save the file.
10. (Optional) Click **Create custom report**.
    - In the **Create custom report** dialog box, enter a display name for the report.
    - (Optional) Enter a report description.
    - Select a compartment in which to store your report.
    - Click **Create custom report**.
11. (Optional) Click **Manage report schedule**.
    The **Manage report schedule** panel is displayed, pre-loaded with either the default or modified schedule.
    a. (Optional) In the **Schedule report name** box, enter a report name.
    b. Select a compartment to store the reports generated by the schedule.
    c. For **Report format**, select **PDF** as the output.

d. Select a **Schedule frequency**.
   - If you select weekly, select the day of the week in the **Every** field.
   - If you select monthly, select the day of the month in the **Day** field.

e. In **Time (in UTC)**, select a schedule time

f. Click **Save schedule**

12. Click **Show Advanced SCIM Query Builder**.

a. Use the provided filter builder and dropdowns to type in your filter(s). Advanced filtering uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:
   - `co`: matches resources with an attribute that contains a given string
   - `eq`: matches resources with an attribute that is equal to a given value (not case sensitive)
   - `eq_cs`: matches resources with an attribute that is equal to a given value (case sensitive)
   - `ew`: matches resources with an attribute that ends with a given string
   - `ge`: matches resources with an attribute that is greater than or equal to a given value
   - `gt`: matches resources with an attribute that is greater than a given value
   - `in`: matches resources with an attribute that is equal to any of given values in list
   - `le`: matches resources with an attribute that is less than or equal to a given value
   - `lt`: matches resources with an attribute that is less than a given value
   - `ne`: matches resources with an attribute that is not equal to a given value
   - `not_in` : matches resources with an attribute that is not equal to any of given values in list
   - `pr`: matches resources with an attribute if it has a given value
   - `sw`: matches resources with an attribute that starts with a given string

   Operators can be grouped using parentheses to specify the order.

   Filters can also be combined using logical operators such as `and` and `or`.

> **Note:**
>
> If you have any basic filters currently applied they will appear in the query builder as well.

b. Click **Apply**.

View Custom Reports

On the **Custom reports** tab, you will see all predefined reports that have been customized and saved.

1. Under **Security center**, click **Security assessment**.

2. Under **Related resources**, click **Assessment reports**. The Security assessment reports page is displayed.
3. (Optional) Narrow the scope of the reports by using **List scope**.
   a. Select a compartment you have access to from the **Compartment** list.
   b. Select or deselect **Include child compartments**. If you select the root compartment and allow the default **Include child compartments**, then child compartments where you have required privileges are included.
4. (Optional) Narrow the scope of the reports by using **Filters**.
   a. Select a target database from the **Target Database** list.
5. View the list of available security assessment reports in the table.
   Within the **Custom reports** tab, you will see the list of custom reports. The table includes the **Report name**, **State**, **Created time**, **Description**, **Report schedule**, and **Latest report**.

View Assessment History

You can view the history of assessments for a specific target database or for all target databases.

View the Assessment History for a Target Database

Security Assessment provides a view of all assessment reports for a single target database. To access this view, first open the latest assessment report and then use the **View History** option.

1. From the **Security Assessment** page, click the **Target Summary** tab.
2. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**.
5. Click **View History**.
6. From the **Compartment** drop-down list, select the compartment that contains the assessment reports. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not include assessment reports for your target database that are saved to the child compartments.
   The **Assessment History** page lists all of the assessment reports for the target database that are contained in the selected compartment and child compartments (if selected). The list includes both auto-generated and saved reports. For each assessment report listed in the table, you can **View the Details** page by clicking on the link. You can also **Set the assessment as Baseline** from the details page.

> **Note:**
>
> The **Created time** for a baseline will display the date and time when the first baseline was set for any target in the current compartment. It is not necessarily the date and time the target specific baseline you are viewing was created.

View the Assessment History for All Target Databases

On the **Assessment History** page, you can view assessments for all target databases within the compartments that you have selected and where you have the required privileges.

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Assessment History**.
3. From the **Compartment** drop-down list, select the compartment that contains the assessment that you wish to view.
   - Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list assessments located in child compartments.
   - If you select the root compartment and allow the default **INCLUDE CHILD COMPARTMENTS**, then child compartments where you have the required privileges are included.
4. (Optional) Under **Filters** select a time period from the **Time Period** list to narrow the lists of reports.
   The selected time period will be displayed in the sub-title of the page.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the lists of reports.
6. View the list of assessments in the table.
   The table includes the target database name, assessment name (which is a link to the assessment), whether or not the assessment is a baseline, when the assessment was created, the state of the assessment (Succeeded or Failed), and the number of high, medium, low, advisory, evaluate, and deferred risk findings in the assessment.

> **Note:**
>
> The **Created time** for a baseline will display the date and time when the first baseline was set for any target in the current compartment. It is not necessarily the date and time the target specific baseline you are viewing was created.

View the Risk Modification Report

You can view a report that details all the findings for a target database where the risk was modified from the risk level designated by Oracle. The report includes if the risk level has been adjusted to any other risk levels (high, medium, low, evaluate, or pass) or if the risk has been deferred, the expiration date, the last updated time, and who modified the risk.

To view the Risk modication report:

1. Under **Security center**, click **Security assessment**.
2. From the **Security Assessment** page, click the **Target Summary** tab.

3. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

   > **Note:**
   >
   > The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The Security Assessment Details page is displayed, showing you the latest assessment report for your target database.
6. Under **Resources**, select **Risk modification report**.
   The Risk modification report displays the finding, original risk, modified risk, deferred risk, justification, expiration date, last updated time, and the user who made the modification.
7. (Optional) Filter the report by clicking **+ Add filter**.

Related Topics

- Adjust the Risk Level of a Risk Finding

Manage Security Assessments

You can refresh, copy, move, delete, or rename an assessment.

Oracle Data Safe provides these tools for managing Security Assessments:

Refresh the Latest Assessment

1. From the **Security Assessment** dashboard, click the **Target Summary** tab.
2. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the row in the table for your target database, and click **View Report**.

   The latest Security Assessment report for your target database is displayed.
5. At the top of the page, click **Refresh** Now.

   The **Refresh Now** window is displayed.
6. (Optional) In the **Save Assessment** box, enter a name for the report.
7. Click **Refresh Now**.

   The latest assessment report for the target database is updated and saved as the specified name.

Save a Copy of the Latest Security Assessment

You can save a copy of the latest assessment for a target database under a new name in a compartment of your choice. This feature does not create a new assessment. It only saves a copy of the latest assessment. One use case for this feature may be the need to share the security evaluation results with other lines of business that do not have access to the assessed target's compartment.

You can save a copy of the last assessment only. You cannot save a copy of a saved assessment.

If you do not want to refresh the latest assessment with updated findings then follow these steps:

1. Under **Related resources** on the **Security assessment** page, click **Assessment history**.

   The **Security assessment history** page is displayed.
2. Select the compartment that contains the assessment. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to not list assessments located in the child compartments.
3. Click **Save latest assessment as**.

   The **Save latest assessment** window is displayed.
4. From the **Target database** drop-down list, select the name of your target database.
5. In the **Assessment name** box, accept the default name for the new copy of the assessment or enter another name.
6. (Optional) In the **Saved assessment description** box, describe the assessment.
7. From the **Saved assessment compartment** drop-down list, select the compartment to which you want to save the assessment.
8. Click **Save latest assessment**.

If you would like to refresh the latest assessment before saving a copy, then follow these steps:

1. On the **Security assessment** page, click the **Target summary** tab.
2. (Optional) Under **Filters** select a target database from the **Target Databases** list to narrow the scope of displayed metrics and charts.
3. In the **Target database** column, find your target database.
4. In the **Last assessed time** column, click **View report**.
5. Click **Refresh now**. The Refresh now panel appears.
6. In the **Saved latest assessment** field, you see that a new name is preselected for the copy. You can accept this name or enter another name.
7. Click **Refresh now**.
   The page then shows the status `UPDATING`. Do not leave the page until the status changes to `SUCCESS`.

Move an Assessment

You can move a saved security assessment (with the exception of the latest assessment) to another compartment. Links to all saved assessments are provided on the Assessment History page.

1. Under **Security center**, click **Security assessment**.
2. Under **Related resources** on the left, click **Assessment history**.
3. Click the report that you want to move to another compartment.
   The report is displayed.
4. From the **More actions** menu, select **Move resource**.
   The **Move resource** dialog box is displayed.
5. From the drop-down list, select a destination compartment.
6. Click **Move resource**. The audit profile is moved immediately.

Change the Name of a Security Assessment

On the **Assessment Information** tab for a security assessment, you can change the auto-generated name of the assessment to a name that has specific meaning for your organization. You and other users can then more easily identify assessments. For example, you could change the auto-generated name of the security assessment `SA_1631303036184` to `SA_main_compartment6_db15a`. It is advisable to include a segment that indicates the assessment is a security assessment, such as the `SA_` prefix in the auto-generated assessment name.

1. From the **Security Assessment** page, click the **Target Summary** tab.
2. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The **Security Assessment Details** page is displayed, showing you the latest assessment report for your target database.
5. Click the **Assessment Information** tab to view details about the assessment.
6. At the **Name** field (first field at the top) click the pencil icon. Change the name and then click the save icon.

   The page may take a few moments to process the change and display the update. When the status under the large SA icon is `SUCCEEDED`, you should see the new name.

Delete an Assessment

You can delete any assessment except for the latest assessment of a target database.

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources** on the left, click **Assessment History**.
3. Click the name of the assessment that you want to delete.
   The report is displayed.
4. From the **More Actions** menu, select **Delete**.
   The **Confirm** dialog box is displayed asking you to confirm the deletion.
5. Click **Delete** to confirm.

This removes the assessment from the Assessment History.

Schedule Security Assessments

Security Assessment has two schedule types: LATEST and SAVED.

There is a default schedule that controls when the latest assessment for your target runs (referred to as `LATEST` schedule). You can rename or update this schedule. You cannot delete it.

Additionally, you can create a custom schedule (referred to as a `SAVED` schedule) to periodically save a copy of the latest assessment for your target database. You can rename, update, or delete `SAVED` schedules.

> **Important:**
>
> When you create or modify schedules, enter all schedule times in UTC (Coordinated Universal Time). Base your schedules on the UTC offset for the region where your tenancy is hosted.

Schedule to Save the Latest Security Assessment

You can create a schedule to periodically save a copy of the latest security assessment for your target database to a compartment of your choice.

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Schedules**. The **Schedules** page is displayed.
3. Click **Add Schedule**. The **The Add Schedule To Save an Assessment** panel is displayed.
4. From the **Target Database** drop-down list, select the target database for which you want to create the schedule.
5. In the **Schedule Name** box, enter a name for the schedule.
6. From the **Schedule Compartment** drop-down list, select the compartment to which you want to save the schedule.
7. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
8. If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
9. If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
10. In the **Time** box, enter a UTC time in the `hh:mm aa` format. Alternatively, click the **Time** box and select a time from the drop-down list.
11. Click **Add Schedule**. The **Schedule Details** page is displayed. The schedule is created when the status reads `SUCCEEDED`.

Each time a copy of the latest assessment is saved, the copy is listed in the Assessment History.

Update a Security Assessment Schedule

You can update a security assessment schedule from two locations in Oracle Data Safe. One location is from the Schedule Details page and the other is from the Security Assessment Details page. Select the appropriate tab below to see the steps for updating a schedule from your desired location.

From the Schedule Details Page

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

   > **Note:**
   >
   > The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Update Schedule**.
   The **Update Schedule** window is displayed.
8. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
   - If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
   - If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
9. In the **Time** box, enter a UTC time in the format `hh:mm ss`. Alternatively, click the **Time** box and select a time from the drop-down list.
10. Click **Update Schedule**.

The schedule is updated when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. From the **Security Assessment** page, click the **Target Summary** tab.

2. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The Security Assessment Details page is displayed, showing you the latest assessment report for your target database.
5. Click the **Assessment Information** tab to view details about the assessment.
6. Click **Update Schedule**.
   The **Update Schedule** window is displayed.
7. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
   - If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
   - If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
8. In the **Time** box, enter a UTC time in the format `hh:mm ss`. Alternatively, click the **Time** box and select a time from the drop-down list.
9. Click **Update Schedule**.

The schedule is updated when the status shown on the page is `SUCCEEDED`.

Stop a Security Assessment Schedule

- From the Schedule Details page
- From the Assessment Details page

From the Schedule Details page

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters** select a target database from the **Target Databases** list to narrow the scope of displayed metrics and charts.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Stop schedule**.
8. Click **Yes** in the confirmation dialog.

The schedule is stopped when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. From the **Security Assessment** page, click the **Target Summary** tab.
2. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The Security Assessment Details page is displayed, showing you the latest assessment report for your target database.
5. Click the **Assessment Information** tab to view details about the assessment.
6. Click **Stop schedule**.
7. Click **Yes** in the confirmation dialog.

The schedule is stopped when the status shown on the page is `SUCCEEDED`.

Start a Previously Stopped Security Assessment Schedule

From the Schedule Details page

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Start schedule**.
   The target database will get assessed again periodically according to the same schedule that was previously defined, by default this is weekly. If you would like to update the schedule see, Update a Security Assessment Schedule.

The schedule is started when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. From the **Security Assessment** page, click the **Target Summary** tab.
2. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The Security Assessment Details page is displayed, showing you the latest assessment report for your target database.
5. Click the **Assessment Information** tab to view details about the assessment.
6. Click **Start schedule**.
   The target database will get assessed again periodically according to the same schedule that was previously defined, by default this is weekly. If you would like to update the schedule see, Update a Security Assessment Schedule.

The schedule is started when the status shown on the page is `SUCCEEDED`.

Delete a Security Assessment Schedule

You can delete a `SAVED` schedule from the **Schedule Details** page. You cannot delete the `LATEST` schedule, which generates the latest assessment for a target database.

1. Under **Security Center**, click **Security Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains the schedule that you want to delete. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments.
4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
6. In the table listing all of the schedules, click the name of the schedule that you want to delete.
   The **Schedule Details** page is displayed.
7. Click **Delete**.
   A Confirm dialog box is displayed asking you to confirm the deletion.
8. Click **Delete** again to confirm.
   The schedule is permanently deleted.

Compare Security Assessments

For target database, you can generate a comparison report that shows the differences between an assessment and the baseline or between any two assessments of the target. This report identifies the security drift that has occurred between the time of the two assessments.

Overview of Security Assessment Comparison

There are two ways to compare security assessments:

- Compare a saved security assessment with the baseline. In this case, you need to set one of your security assessments as the baseline.
- Compare the latest security assessment with a saved assessment from the Assessment History.

After you have fixed any significant findings in an assessment you can either wait for the next scheduled assessment or use the **Refresh Now** option to immediately refresh the assessment. You can then recheck the assessment to confirm that the fixes have successfully reduced the risks in the target database. If you are satisfied that this assessment represents an optimal security posture, you can set it as the baseline to compare against other assessments.

For example, let's say that in January you spent a month addressing all of the findings for your target database. On February 1, all of the risks have been resolved. You may then want to set the security assessment from February 1 as your new baseline. First, refresh the target database assessment to ensure the fixed findings no longer appear as risks. Then you can set

the February 1 assessment as the baseline. From that point on, you are able to observe any security drift since the February 1 assessment.

The baseline can be the latest assessment, but this is not required. You can also go back into Assessment History and set an older assessment as the baseline.

If you have set a baseline for a target, then on the **Security Assessment** page you can check for any drift from the baseline assessment. Click the **Target Summary** tab. If there has been any security drift in a target database, then the **Deviation From Baseline** column in the summary alerts you to the deviation. This column also tells you whether or not a baseline has been set for the target database.

Summary of Tasks to do before Setting a Baseline

1. Assess the target database.
2. Identify the risks and review.
3. Fix the findings that need to be addressed.
4. Assess the target database again.
5. If the new security assessment shows fewer or no risks, then set it as the baseline.

Structure of a Comparison Report

A Comparison Report consists of a summary table and a details table.

The summary table helps you to identify where the risk level changes are occurring on your target database and whether the risk levels are increasing, decreasing, or staying the same. The details table describes the changes on the target database. The risk levels are categorized as High, Medium, Low, Advisory, Evaluate, Deferred, and Pass. The categories represent types of findings, which are User Accounts, Privileges and Roles, Authorization Control, Data Encryption, Fine-Grained Access Control, Auditing, and Database Configuration. You can view the number of new risks added, the number of risks remediated (removed), and the number of risks that have changed to a different risk level (modified). The change value is the total count of new, remediated, and modified risks on the target database for each category/risk level. The green color is used to indicate a positive change whereas the red color indicates the change needs your attention.

In the details table, you can view the risk level for each change, the findings category to which the change belongs, and a description of the change. The Comparison column is important because it provides explanations of what is changed, added, or removed from the target database since the baseline report was generated. The column also tells you if the change is a new risk or a remediated risk.

Set the Latest Assessment or a Saved Assessment as the Baseline for a Target Database

You can set the latest security assessment or an archived security assessment for a target database as a baseline.

1. Under **Security Center**, click **Security Assessment**.
2. From the **Security Assessment** page, click the **Target Summary** tab.
3. From the **Compartment** drop-down list, select the compartment that contains your target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. In the **Target Summary** table, locate your target database and then click the **View Report** link to open the latest assessment report.
   The **Security Assessment Details** page shows the latest assessment.
6. To set the latest assessment as the baseline, do the following:
   a. Click **Set as Baseline**.
      The **Set as Baseline** dialog box is displayed asking you to confirm setting the latest saved assessment report as a baseline.
   b. Click **Yes** to confirm.
7. To set an earlier assessment as the baseline, do the following:
   a. Click **View History**.
   b. Review the risk findings for the listed assessments and identify a particular assessment to use as the baseline.
   c. Click the name of the assessment.
   d. Click **Set As Baseline**. The **Set as Baseline** dialog box is displayed asking you to confirm setting the assessment report as a baseline.
   e. Click **Yes** to confirm.

> **Tip:**
>
> You can also set an assessment as the baseline through the **Assessment History** page.
>
> 1. Navigate to the **Security assessment** page.
> 2. Under **Related resources**, click **Assessment history**. The **Security assessment history** page is displayed, listing all previous auto-generated assessments.
> 3. (Optional) Under **Filters** select a time period from the **Time period** list to narrow the scope of displayed metrics and charts.
> 4. (Optional) Under **Filters** select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
> 5. Click an assessment name to view its details.
> 6. Click **Set as baseline**. The **Set as baseline** dialog box is displayed asking you to confirm setting the assessment report as a baseline.
> 7. Click **Yes** to confirm.

Compare the Latest Assessment with the Baseline

You can compare the latest security assessment with the baseline. To do this, open the latest assessment report and use the **Compare with Baseline** feature. Setting a baseline assessment report is a prerequisite.

1. Under **Security Center**, click **Security Assessment**.

2. From the **Compartment** drop-down list, select the compartment that contains your target database. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list target databases in the child compartments.
3. Click the **Target Summary** tab.
4. Open the latest assessment report. To do this, in the **Target Summary** table, locate the line for your target database, and click **View Report** in the **Last Assessed On** column.
   The **Security Assessment Details** page is displayed, showing you the latest assessment report for the target database. On the left under **Resources**, you now have two options to compare assessment reports.
5. Under **Resources**, click **Compare With Baseline**.
   A **Comparison With Baseline** section is displayed on the page. If a previous comparison was done, the latest Comparison report is displayed in the section, including the name and creation date of the baseline report.

   > **Note:**
   >
   > The **Created time** for a baseline will display the date and time when the first baseline was set for any target in the current compartment. It is not necessarily the date and time the target specific baseline you are viewing was created.

6. To do a comparison, click **Compare Now**.
   The Comparison report is displayed.
7. View the Comparison report.
   Review the number of findings per risk category for each risk level. Categories include `User Accounts`, `Privileges and Roles`, `Authorization Control`, `Data Encryption`, `Fine-Grained Access Control`, `Auditing`, and `Database Configuration`.

   You can identify where the changes have occurred on your target database by viewing cells that contains `Modified`. The number represents the total count of new, remediated, and modified risks on the target database.

Compare a Saved Security Assessment With the Latest Assessment

You can compare any saved assessment with the Latest Assessment of the same target database.

1. Under **Security center**, click **Security assessment**.
2. Click the **Target summary** tab.
3. From the **Compartment** drop-down list, select the compartment that contains your target database. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list target databases in the child compartments.
4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. Open the latest assessment report for your target database. To do this, in the **Target summary** table, locate the line for your target database, and click **View report** in the **Last assessed time** column.
   The **Security Assessment Details** page is displayed, showing you the latest assessment report for the target database.
6. Under **Resources** on the left, click **Compare Assessments**.
   The **Security Assessment Details** page updates to include a comparison section.

7. (Optional) If the assessment report that you want to select is located in a different compartment than the one that is shown, click **Change Compartment**, and select a different compartment.
8. From the **Select Assessment** drop-down list, select an assessment report. .
9. Click **Compare Now**.
   While Security Assessment is comparing the two reports, you see the message `Comparison in Progress`. When the comparison is completed, the report is displayed on the same page.

   If there are no differences between the reports, the message **Assessments Are Identical** is displayed in the **Finding** column.

Generate and Download a PDF or XLS Report

You can generate and then download a PDF or XLS-formatted report based on the latest assessment or baseline assessment for a target database.

1. View the latest or baseline assessment for a target database.
2. From the **More Actions** menu, select **Generate Report**.
   The **Generate Report** dialog box is displayed.
3. Select the report format that you want to use. You can choose either PDF or XLS.
4. Click **Generate Report**.
5. Wait for the report to complete, then click **Close**.
6. You can then pull down **More Actions** again and click **Download Report**.
7. Save the report to your local computer.

> **Note:**
>
> There is no option to generate a report from an assessment other than the latest or baseline assessment.

Create and Modify Event Notifications in Security Assessment

You can create and modify event notifications in Security Assessment.

Creating Event Notifications for Security Assessment

In Data Safe you can create event notifications for Security Assessment related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **Security assessment**.

2. Click the **Notifications** tab.
3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Security Assessment Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

   > **Note:**
   >
   > This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
12. Click **Create notification**.

Modifying Event Notifications For Security Assessment

After creating event notifications in Security Assessment in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **Security assessment**.
2. Click the **Notifications** tab.
3. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **Security assessment**.
2. Click the **Notifications** tab.
3. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

3

User Assessment

This section discusses how to assess user security by using the User Assessment feature in Oracle Data Safe.

User Assessment Overview

The User Assessment feature in Oracle Data Safe helps you to identify highly privileged user accounts that could pose a threat if misused or compromised.

About User Assessment

Knowing which users have access to sensitive data is essential to managing risk. Which database accounts have powerful roles, such as Database Administrator, Database Vault Administrator, or Audit Administrator? Who can make changes that seriously impact the system, access sensitive data, or grant access to unauthorized users? Is there a risk of attackers taking over some user accounts because the passwords have not been changed in a long time? Is password complexity being checked for all user accounts? If not, for how many users? The User Assessment feature in Oracle Data Safe answers these questions and more to help you identify highly privileged user accounts that could pose a threat if misused or compromised. Administrators can then deploy appropriate security controls and policies.

User Assessment reviews information about your users in the data dictionaries on your target databases and then calculates a risk score for each user, based on system privileges and role grants. For example, it displays the user types, how users are authenticated, the password policies assigned to each user, and how long it has been since each user has changed their password. With this information, you can decide whether to implement more restrictive password policies, use Oracle Database Vault, or add other security controls to further limit user access, if needed.

After you register a target database, Oracle Data Safe automatically runs a User Assessment for that target database. The User Assessment feature is supported for all database types and versions currently certified by Oracle Data Safe. To view audit records for users in User Assessment, you must start audit data collection in Activity Auditing for your target database.

For all registered target databases, User Assessment automatically generates an assessment once per week and saves a copy of it to the history. This assessment is referred to as the "latest" assessment. If needed, you can modify its schedule. You also have the option to create a schedule that saves a copy of the latest assessment to a different compartment and with a different name.

User Assessment lets you refresh the latest assessment at any time by using the Refresh Now option. After the latest assessment is refreshed, Security Assessment saves the assessment to the history and also overwrites the latest assessment. To monitor security drift on your target database, you can compare two assessments. You can define a baseline assessment and compare other assessments to it, or, you can compare two selected assessments. Lastly, you can generate a PDF or XLS report from an assessment.

The following are use cases for the User Assessment feature:

- Quickly assess your databases to learn about the existing user accounts, their privilege and role grants, and the potential risk a compromised or misused account would pose.
- Identify highly privileged users.
- Identify system privileges and role grants that could be unnecessary.
- Identify dormant accounts.
- Identify users with stale passwords.
- Review existing user profiles, their password parameters including their password complexity verification function.
- Identify users and profiles without password governance policies.
- Identify which profiles are assigned to which users.
- Identify discrepancies in user profiles password attributes across multiple targets.
- Promote database security best practices.
- Monitor security drift by comparing an assessment against a baseline.

A user assessment shows all registered Oracle Data Safe target databases in a selected compartment. You have the option to include all child compartments of the selected compartment. This is the scope of the assessment. If you select the root compartment and include child compartments, then the assessment shows all assessments across all compartments in the tenancy.

User Assessment Compared to Security Assessment

User Assessment and Security Assessment are complementary features of Oracle Data Safe. While Security Assessment analyzes risks pertaining to database configuration, User Assessment focuses exclusively on the inherent risk factors in user access to the database.

Understanding Potential Risk in User Assessment

Potential Risk Levels in User Assessment

Each user is assigned a potential risk level that is determined by their granted roles and privileges.

Potential Risk Level	Description
Critical	• Scope: database level. • Impact: database availability and integrity. • Has direct read/modify/copy access to data. • Can bypass or alter security policies. • Cleanup audit data. • Malicious activity possible.

Potential Risk Level	Description
High	• Scope: feature level. Potential for malicious activity is limited to a smaller scope than that of a user in the Critical category. • Ability to read/modify/copy data indirectly through use of the corresponding privileges. This requires more effort to accomplish than the direct access capability of a user in the Critical category. • Can degrade performance at a query level – alter/drop SQL profiles or SQL translation profiles. • Allows key management. • Can create, alter, or drop database profiles.
Medium	• Has privileges which have a large scope, but do not have serious effects. For example, a user with ALTER RESOURCE COST privilege can set costs for user sessions.
Low	• Scope: Privileges specific to the grantee.

> **Note:**
>
> Risk levels in User Assessment and System Assessment are different. User Assessment designates some user risk factors as CRITICAL. This designation is not used in Security Assessment. Likewise, the ADVISORY and EVALUATE risk levels in Security Assessment are not part of User Assessment.

User Types

User Assessment categorizes users into different user types. These are the possible user types:

- Admin Privileged - The user has administrative privileges such as, `SYSDBA`, `SYSOPER`, `SYSBACKUP`, `SYSDG`, `SYSKM`, or `SYSRAC`.
- Application - The user is an Oracle E-Business Suite Applications (EBS) or Fusion Applications (FA) user.
- Privileged - The user is a privileged user. Users that pose a potential risk level of High or Critical are flagged as privileged.
- Schema - The user is `EXPIRED & LOCKED`, `EXPIRED`, `LOCKED`, or a schema-only account (whose authentication type is `NONE`).
- Non-privileged - The user is a non-privileged user. A non-privileged user is a user who does not have elevated access rights and, thus, is not classified under any specific user type. Their granted privileges are limited and cannot cause any system-wide impact. Such a user cannot make changes at the database or user level, nor can they impact objects not owned by them.

Scope

You can set the scope of your view of User Assessment to the root compartment alone or root with all of its child compartments or to any compartment under root with or without that compartment's child compartments.

When you look at potential risk findings and target database users in User Assessment you can set the scope to root with its child compartments to review the overall security posture of your tenancy. You can also set the scope to focus on a specific compartment of interest.

> **Note:**
>
> It's important to remember that within the selected scope, your view within User Assessment is determined by the privileges your account has been granted in OCI.

Risk Summary and Target Summary

On the User Assessment page, the Risk Summary tab gives you a broad look at all of the current potential risk findings in the selected scope.

The Target Summary tab lets you focus on a specific target database and all of the users within that database.

User Profiles

User Profile details are gathered by a User Assessment run. Managing user profiles across multiple Oracle databases can be challenging as the number of databases and users increases. Multiple databases make it hard to spot inconsistencies in these profiles. For example, a specific user profile can have password parameters set differently in various databases, leading to non-compliance with regulatory requirements. As the number of users and potentially the number of profiles grow, managing them can become increasingly complex and time-consuming, especially if managing them at scale for multiple databases. User Profiles helps to spot inconsistencies and work towards unifying user profiles across all databases in your fleet.

Terms in User Assessment

- On demand (**Refresh Now**) Assessment
  You can click the **Refresh Now** button on any assessment to rerun it immediately against the selected target database.
- Scheduled Assessment
  A weekly user assessment is automatically scheduled for every registered target database. You can change the schedule to a different time and/or a daily or monthly interval.
- Latest Assessment
  The most recent assessment completed (either on demand or scheduled) for the selected compartment. Each new assessment becomes the Latest assessment.
- Saved Assessment
  A copy of the latest assessment saved to a compartment of your choice. The copy is listed in the history.
- Assessment History
  The archive of all saved assessments of a target database.
- Baseline

An assessment that you can designate as the standard for a target database. When an assessment runs, in addition to finding potential risks the job tells you whether or not there is any deviation (security drift) from the findings in the baseline. There is a **Set as Baseline** option in each assessment.

User Assessment Workflow

This is an end-to-end walkthrough of User Assessment functionality for new users, not a fixed procedure.

When you register a target database in Oracle Data Safe, a user assessment is run on the database automatically. So the first time you check the User Assessment page after registration, assessment data is already there. By default, this data is refreshed on a weekly schedule at the same time as when the registration was completed. This workflow explains how to view that data.

1. Check that your target database that you want to assess are registered and that you have assigned the necessary permissions in IAM.
2. In Security Center, click **User Assessment**. On the User Assessment dashboard, check the charts and the **Risk Summary** and **Target Summary** to evaluate the overall security posture of your databases. Set the scope of data you want to see. The scope can encompass the databases in the root compartment alone or the root and everything under it. It can also be limited to any selected compartment, with or without its child compartments. From there, you can drill down for more data.
3. There are several drill down paths you can follow:
   - Click the **Risk Summary** tab and then click through the **Potential Risk** links. For example, you can click on **Critical** and see another set of charts, which summarize the critical roles held among users in the database, date of last password changes, and last login times among users at the Critical potential risk level. On the same page you can review the **Critical Potential Risk Details** table which provides more information about each user account at the critical level.
   - Also from the User Assessment page, you can click the **Target Summary** tab to get a different perspective on the potential risk findings. This tab shows you the target databases in the selected scope, the number of users per database at each potential risk level, the number of critical roles held with each database, and other factors. This table also shows you whether or not you have run a comparison of the latest assessment to the baseline assessment and if there has been deviation (security drift) from the baseline. You can click **View Report** for any target database to view latest User Assessment of the database.
4. Run or schedule user assessments.
   - Use the **Refresh Now** button to immediately run a user assessment. The assessment is added to the Assessment History. **Refresh Now** also refreshes the latest user.
   - Modify the schedule for the weekly User Assessment job. The job updates the latest report view and also saves a copy to the history. If needed, you can also specify that the reports be saved under a different name or to a different compartment. This option is helpful if you want to share reports with users from other lines of business.
5. Compare user assessments to determine if there is any security drift.
   - You can set the latest assessment or a saved assessment as the baseline.
   - When you compare assessments, User Assessment generates a comparison report.
6. Adjust the schedules of your security assessments to suit the needs of your organization.

7. Change the names of your user assessments to names that are meaningful to you. The default names that Oracle Data Safe assigns follow this pattern: `UA_<unique number>`. It's helpful to choose your own names. You may want to retain the `UA_` prefix because it will distinguish user assessments from user assessments (`SA_`).
8. Create PDF or XLS versions of you user assessment reports as needed and then download them.
9. Set up event notifications. For example, you can subscribe to the `UserAssessmentDriftFromBaseline` event to be automatically informed if a user assessment differs from the baseline.

Prerequisites for User Assessment

User Assessment requires registered, properly provisioned target databases. Users must be granted specific permissions in IAM.

These are the prerequisites for User Assessment:

- **Register the target databases where you want to run User Assessment.**
  After you register a target database, Oracle Data Safe automatically runs a user assessment for your target database and updates it according to the schedule (once per week by default).
- **For all database types supported by Oracle Data Safe except Autonomous Database, grant the `ASSESSMENT` role to the Oracle Data Safe service account on the target database.**
  An Autonomous Database is automatically provisioned with the equivalent `DS$ASSESSMENT_ROLE` when it is registered as a target database.
- **Obtain either the `view` permission or the `manage` permission on the `user-assessments` resource in IAM (Oracle Cloud Infrastructure Identity and Access Management).**
- **Obtain `read` permission on the `data-safe-work-requests` resource in IAM if you need to set baselines or compare assessments.**
- **Obtain `read` or `use` permission on the `data-safe-security-policy-reports` resource in IAM if you need to view details about the schemas and tables that a user has access to, as well as what privileges the user was granted on these schemas and tables.**

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-assessment-family` in the relevant compartments, which would include permissions on all of the resources above as well as `security-assessments`. See data-safe-assessments-family Resource in the *Administering Oracle Data Safe* guide for more information.

See Also:

The *Administering Oracle Data Safe* guide provides these sections to help with establishing the prerequisites:

- Migrate to Oracle Cloud Infrastructure You can follow the one-time migration procedure described in the guide or you can do the migration manually. The migration described in the guide does not include permissions on the `data-safe-work-requests` resource. Add that resource as needed.
- Grant Roles to the Oracle Data Safe Service Account on Your Target Database describes the roles required for User Assessment and for other Oracle Data Safe features.
- user-assessments Resource provides the policy statement for granting users read permissions on `user-assessments`.
- data-safe-work-requests Resource provides the policy statement for granting users read permissions on `data-safe-work-requests`.

Recommended Before You Start

Oracle recommends you try the *Get Started with Oracle Data Safe Fundamentals* workshop in LiveLabs before you use User Assessment.

The *Get Started with Oracle Data Safe Fundamentals* workshop includes hands-on training for User Assessment. Whether or not you've taken the workshop before, you'll find that the lab for User Assessment provides an up-front familiarity with this feature that makes it easier for you to put it to work in your organization. Consider going through the workshop to learn about User Assessment before you proceed.

Try it now:

Get Started with Oracle Data Safe Fundamentals

Analyze Potential Risk by Using the User Assessment Dashboard

The User Assessment dashboard provides a high-level overview of potential user risk across your target databases. From there, you can drill down to the details of each user assessment.

Navigating to the User Assessment Dashboard

To navigate to the User Assessment dashboard: On the **Overview** page in the Oracle Data Safe service, go to the panel on the left, and under **Security Center**, click **User Assessment**.

A First Look at the User Assessment Dashboard

The User Assessment dashboard contains these components:

- **Potential user risk**, **User roles**, **Last password change**, **Last login**, and **Password expiry date** charts
- **Risk summary** tab
- **Target summary** tab
- **Notifications** tab
- **Related Resources**
- **List Scope**

You can explore key features and workflows with the guided tour option by clicking the "Take the tour" button in the User Assessment dashboard. The dashboard shows you several high-level views of potential risk findings from the latest assessments of the target databases within the selected compartment. The compartment is set under **List Scope** at the bottom of the dashboard. The scope can optionally include child compartments of the selected compartment.

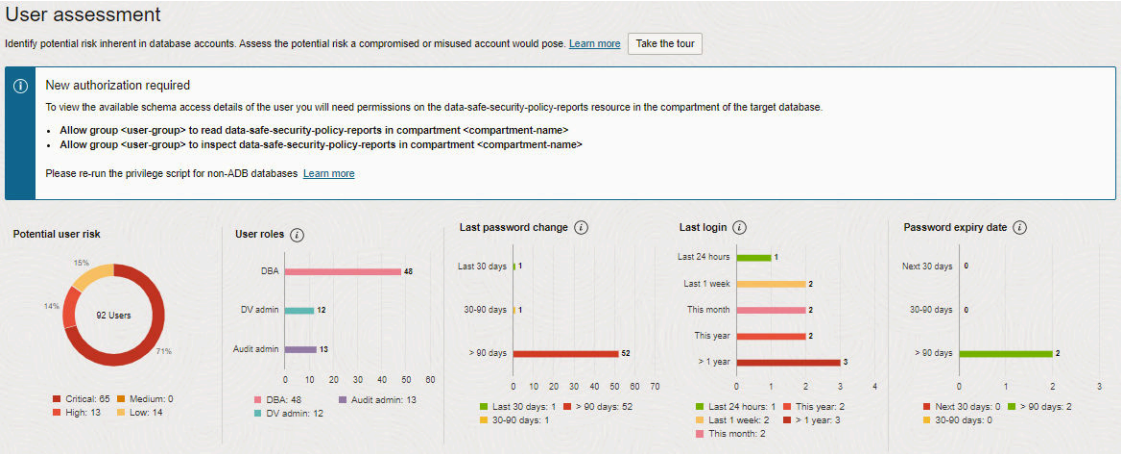
The Potential User Risk, User Roles, Last Password Change, Last Login, and Password Expiry Date Charts

The dashboard provides a set of charts that show you the current user security status at a glance. It also provides Risk Summary, Target Summary, and Notifications tables where you can drill down to get more details about current potential risk factors.

The charts show you the collective potential risk findings from the most recent assessment of each target database in the selected scope.

- The **Potential user risk** chart breaks down the total number of users found and shows the percentage at each potential risk level.
- **User roles** shows the crucial roles held by privileged users in you target databases.
- **Last password change** shows how recently users of the target databases changed passwords.
- **Last login** shows how recently users of the target databases changed passwords.
- The **Password expiry date** chart shows the number of users whose passwords will expire within three distinct time intervals (next 30 days, 30-90 days, and beyond 90 days). Clicking on a bar opens a side panel that lists target databases on the left, showing those databases with users whose passwords expire within that period, and their corresponding latest assessments on the right. From there, you can click an assessment name to open a pre-filtered user assessment report displaying only the affected users in that database.

These charts give you a quick overview about the state of user security for target databases in the compartment. In the example below, you can see that the latest assessment within this scope found a substantial number of users categorized as critical or high risk.



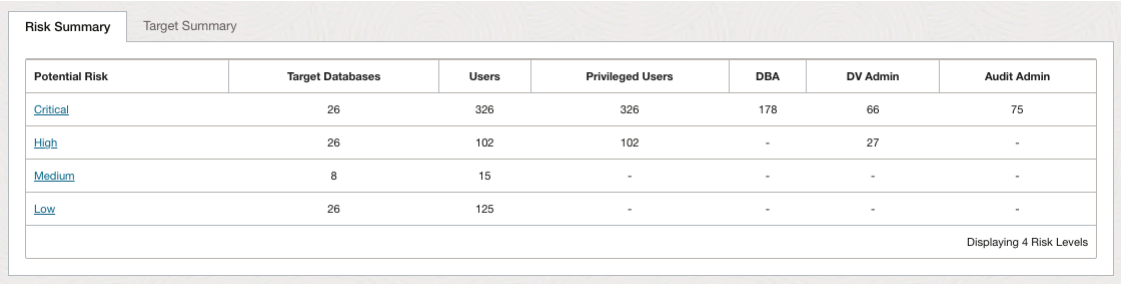
More detail is provided in the tables on the dashboard. In both of these tables, use the links to drill down to more detailed information.

Risk Summary, Target Summary, and Notifications Tables

The dashboard provides three tables – Risk Summary, Target Summary, and Notifications.

The Risk Summary Table

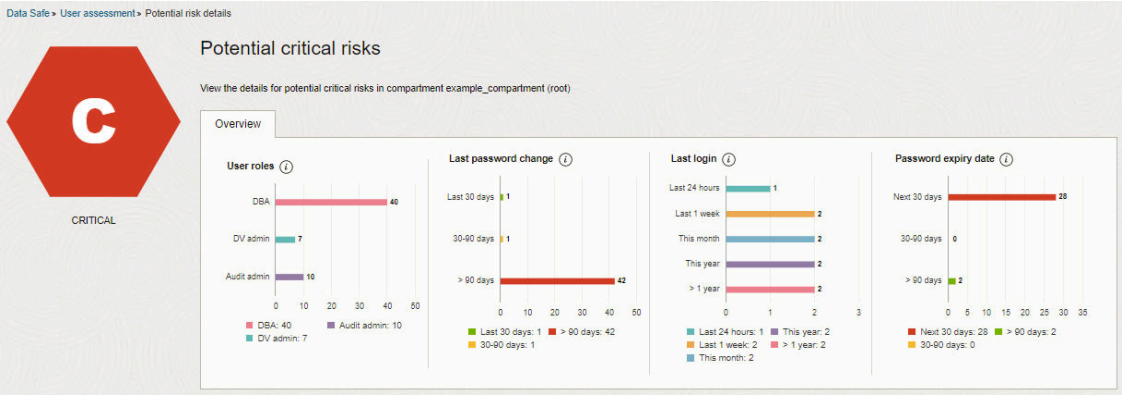
The **Risk Summary** focuses on potential risk levels, where the potential risks were found, the number of users at each potential risk level and the roles held by the total number of users at each potential risk level.



In the **Potential Risk** column, click on a potential risk level to view the users with that potential risk level from all target databases in the selected scope. For example, click **Critical** to view all users marked as **Critical**.

If a user is in the Critical or High potential risk category, this does not mean that the user has performed any inappropriate actions. It means the user has privileges that include access to important database functionality and that in the findings identified by the assessment, the need for such access should be confirmed.

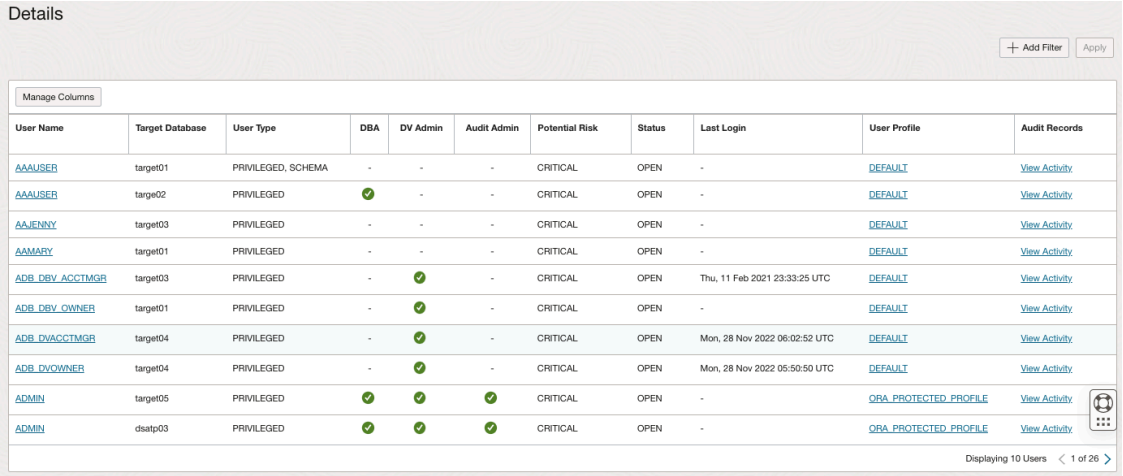
The chart under **Potential Critical Risks** shows the roles held among the body of users considered to be potential critical risks as well as the most recent logins, password changes among these users, and password expiry dates. Clicking on a segment of any chart will automatically filter the **Details** below accordingly. To clear the filter either click outside of a chart or clear the filter in the **Details** section.



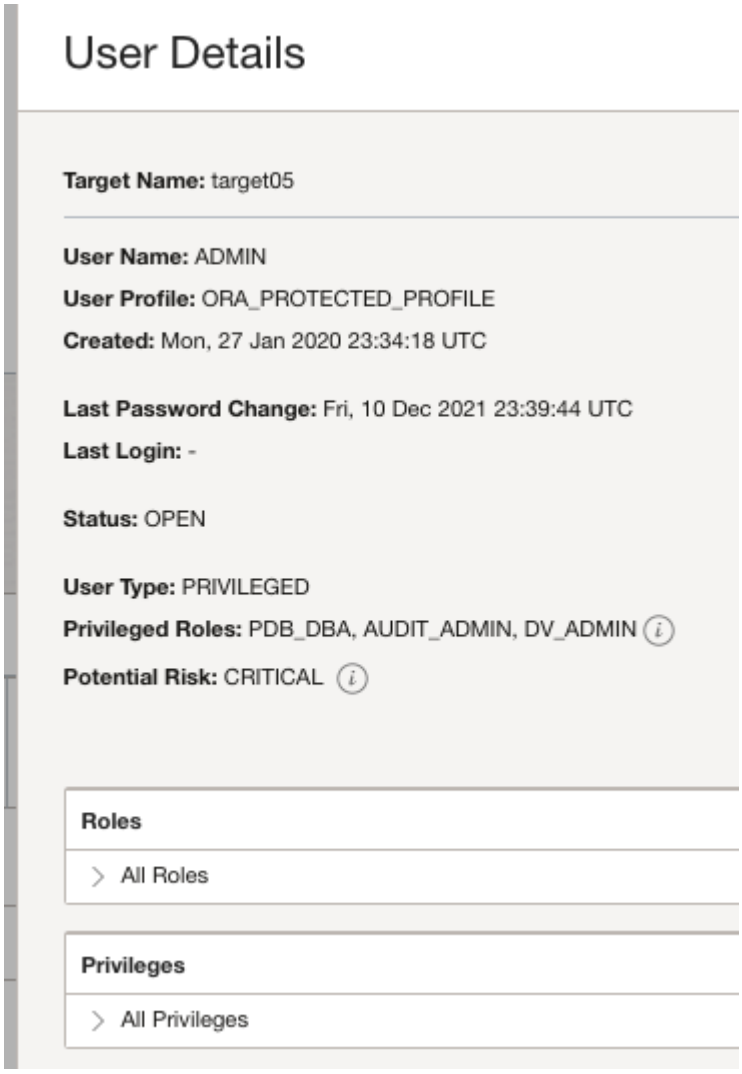
Important:

A malicious actor who acquires access to a user account that is rated as a High or Critical potential risk can have a devastating impact on a database and its data. The actions of highly privileged users should be audited. Their privileges and role grants should be validated.

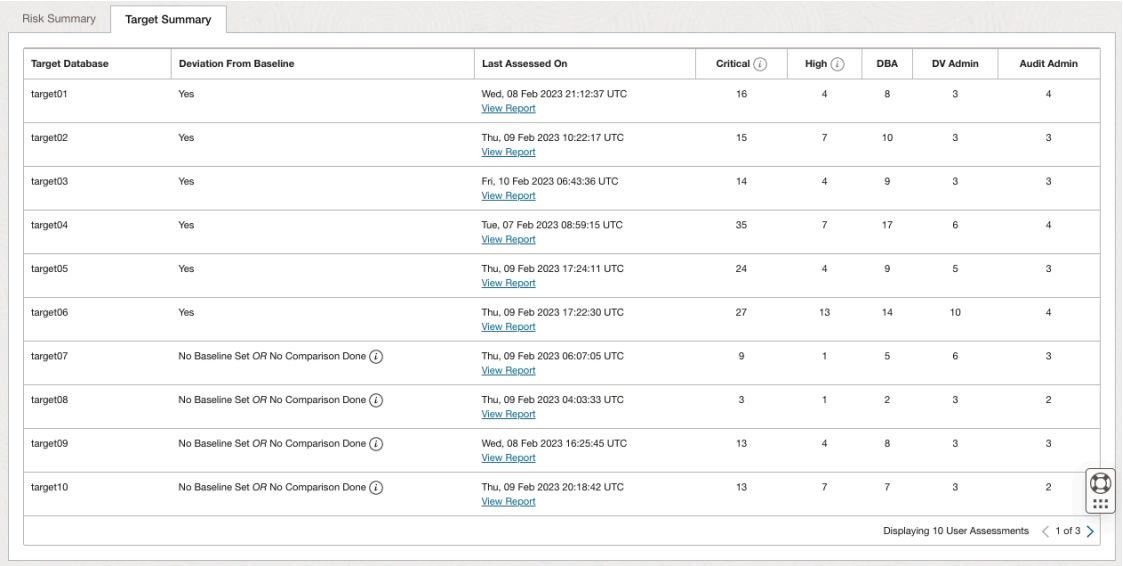
The **Details** table below the charts provides more details on each user. It identifies the database where the user account exists, whether the user is highly privileged or not, what roles they hold, the potential risk level assigned to this finding, current status of the finding, and last login for the user.



Click on the **User Name** to get additional details about the user including the roles and privileges granted to the user. For example:



From the **Risk Summary** tab, click the **Target Summary** tab to shift the focus to each target database, including the findings from the most recent assessment of that database. Oracle Data Safe generates a report for each target database included in an assessment. For any of the target databases listed you can click **View Report** to see the details.



Notifications

The **Notifications** tab shows you what event notifications and subscriptions you have created for User assessment. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show Events that you have created directly within Data Safe. In addition to displaying existing event notifications, you can also create new notifications by using the **Create notification** button. See Creating Event Notifications for User Assessment for more information.

List Scope

List scope is where you set the scope of the lists in the **Risk summary**, **Target summary**, and **Notifications** tabs. It determines which compartments are included in those lists.

You can set the scope of your view of User Assessment to the root compartment alone or root with all of its child compartments or to any compartment under root with or without that compartment's child compartments.

When you look at potential risk findings and target database users in User Assessment, you can set the scope to root with its child compartments to review the overall security posture of your tenancy. You can also set the scope to focus on a specific compartment of interest.

> **Note:**
>
> It's important to remember that within the selected scope, your view within User Assessment is determined by the privileges your account has been granted in OCI.

Viewing an Assessment

Click **View Report** in the Target Summary for comprehensive details about the assessment. This is an interactive report and you can click the buttons under the assessment name (UA_1631303036184 in this case) to make changes:

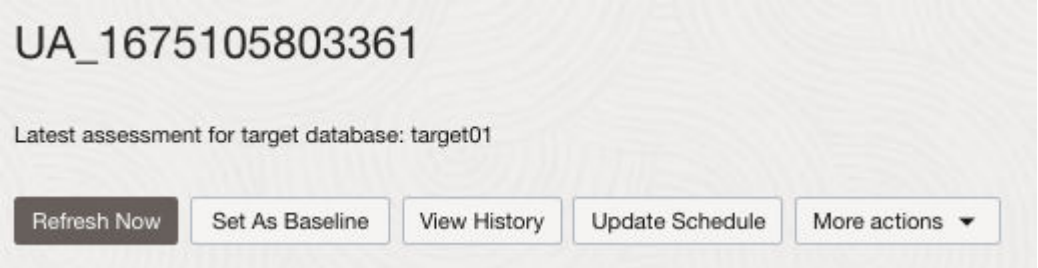
Refresh Now – Rerun this assessment (the assessment of the target database you selected in the Target Summary only, not the assessment of the entire compartment).

Set as Baseline – Make this assessment the baseline for comparison with other assessments of the target database. You may want to refresh the assessment first.

View History – See the reports from past iterations of this assessment.

Update Schedule — Change the schedule of the assessment.

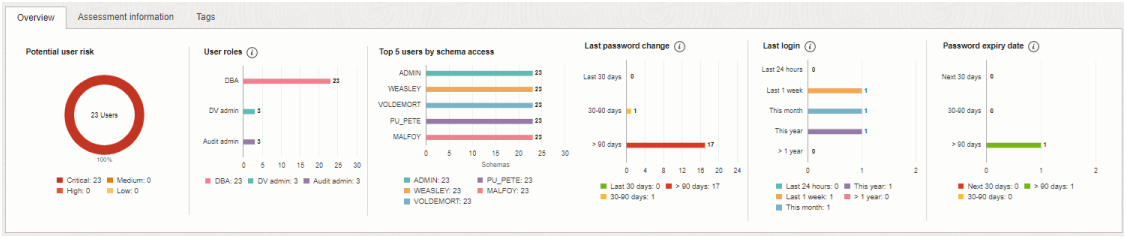
> **Note:**
>
> You can change the auto-generated assessment to more descriptive name at any time. See the Assessment Information tab, which is described further below in this article.



Assessment Overview and Assessment Information

In the **Overview** tab, six charts provide a quick summary of assessment status. In the **Potential user risk** chart below, seven users of the database have some level of potential risk. The **User roles** chart shows the distribution of privileged roles among these users. The **Top 5 users by schema access** chart shows the five users that have access to the most number of schemas. **Last password change** indicates how recently users have changed their password in 90 days or less. **Last login** shows the total number logins into the database. The **Password expiry date** chart displays how many days remain until user passwords expire. Each bar in the chart represents a time range, such as "Next 30 days." Clicking on a bar opens a side panel that lists target databases on the left, showing those databases with users whose passwords expire within that period, and their corresponding latest assessments on the right. From there, you can click an assessment name to open a pre-filtered user assessment report displaying only the affected users in that database.

> **Note:**
>
> There are two reasons why the total count of user differs in these charts. In case of **Last Password Change**, there is no password change data for users created using the NO AUTHENTICATION clause in the database. Such users are not included in the count. In the **Last Login** chart, user accounts of the SCHEMA type are locked and expired. There is no login data for these users and so they are not included in the count.



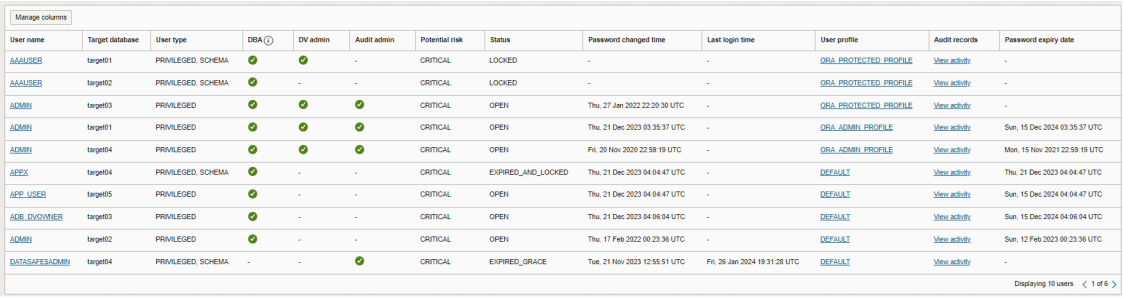
Click the **Assessment Information** tab for key information about the assessment including target database and the configured baseline. **Complies with Baseline** indicates whether or not there are deltas from the baseline assessment that was used for comparison. If you have questions about why the assessment is in or out of compliance with the baseline, you can click on **Baseline** to view the details of the baseline. The pencil icons indicate that you can change the name of this assessment and also change the schedule.

You can change the **Name** of the assessment on this tab and can also change the **Schedule** for automated refreshes of the assessment.

Assessment Details

This table breaks down the summarized data provided earlier in the report into the assessment details collected for each user.

You can click on **User Name** to review the profile of a specific user. If you want to check the database activity of the user, click **View Activity** to view the All Activity audit report.



Manage columns

User name	Target database	User type	DBA	DV admin	Audit admin	Potential risk	Status	Password changed time	Last login time	User profile	Audit records	Password expiry date
AAAUSER	target01	PRIVILEGED, SCHEMA	✓	✓	-	CRITICAL	LOCKED	-	-	ORA_PROTECTED_PROFILE	View activity	-
AAAUSER	target02	PRIVILEGED, SCHEMA	✓	-	-	CRITICAL	LOCKED	-	-	ORA_PROTECTED_PROFILE	View activity	-
ADMIN	target03	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	Thu, 27 Jan 2022 22:20:36 UTC	-	ORA_PROTECTED_PROFILE	View activity	-
ADMIN	target01	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	Thu, 21 Dec 2023 03:35:37 UTC	-	ORA_ADMIN_PROFILE	View activity	Sun, 15 Dec 2024 03:35:37 UTC
ADMIN	target04	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	Fri, 20 Nov 2020 22:59:19 UTC	-	ORA_ADMIN_PROFILE	View activity	Mon, 15 Nov 2021 22:59:19 UTC
APPX	target04	PRIVILEGED, SCHEMA	✓	-	-	CRITICAL	EXPIRED_AND_LOCKED	Thu, 21 Dec 2023 04:04:47 UTC	-	DEFAULT	View activity	Thu, 21 Dec 2023 04:04:47 UTC
APP_USER	target05	PRIVILEGED	✓	-	-	CRITICAL	OPEN	Thu, 21 Dec 2023 04:04:47 UTC	-	DEFAULT	View activity	Sun, 15 Dec 2024 04:04:47 UTC
ADB_DVOWNER	target03	PRIVILEGED	✓	-	-	CRITICAL	OPEN	Thu, 21 Dec 2023 04:06:04 UTC	-	DEFAULT	View activity	Sun, 15 Dec 2024 04:06:04 UTC
ADMIN	target02	PRIVILEGED	✓	-	-	CRITICAL	OPEN	Thu, 17 Feb 2022 00:23:36 UTC	-	DEFAULT	View activity	Sun, 12 Feb 2023 00:23:36 UTC
DATASAFESADMIN	target04	PRIVILEGED, SCHEMA	-	-	✓	CRITICAL	EXPIRED_GRACE	Tue, 21 Nov 2023 12:55:51 UTC	Fri, 26 Jan 2024 19:31:28 UTC	DEFAULT	View activity	-

Displaying 10 users 1 of 6

View User Assessments and Assessment History

There are several ways to view user assessments for your target databases. The latest assessment for a target database is always available from the User Assessment dashboard. The Assessment History lets you view all of the assessments for one or more of your target databases. From there, you can view individual assessments throughout the history.

This article includes the following topics:

View the Latest User Assessment for a Target Database

You can access the latest assessment for an individual target database via the Target Summary tab.

1. From the **User Assessment** page, click the **Target Summary** tab.
2. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The **User Assessment Details** page is displayed, showing you the latest assessment report for your target database
5. At the top of the report, review the set of charts specific to the selected database to get a quick view of the current security posture. The charts show you the collective potential risk findings from the most recent assessment of the selected target database. The **Potential user risk** chart breaks down the total number of potential risks found and shows the total number of users broken down by potential risk level. **User roles** shows the crucial roles held by privileged users in those target databases. **Top 5 users by schema access** shows the five users that have access to the most number of schemas. **Last password change** and **Last login** show the totals for how recently users of the target databases performed those actions, also broken down by percentages. **Password expiry date** shows the number of users whose passwords will expire within three distinct time intervals (next 30 days, 30-90 days, and beyond 90 days). These charts give you a quick overview about the state of user security for the selected target database. You may for example, be able to see right away that the latest assessment found a substantial number of CRITICAL and HIGH potential risk users. In addition, clicking on any of the chart segments will filter the **Assessment Details** accordingly.

6. Click the **Assessment Information** tab to view details about the database and the latest user assessment run on the database, including the baseline assessment (if any) that was used to identify changes in the potential risk level posed by user accounts.
7. (Optional) Click on **Baseline** to view the baseline and then use the browser back arrow to return the **User Assessment Detail**s page.

> **Note:**
>
> The **Created time** for a baseline will display the date and time when the first baseline was set for any target in the current compartment. It is not necessarily the date and time the target specific baseline you are viewing was created.

8. Scroll down to **Assessment Details**, where you can drill down to get more details about current risk factors. Here you see a profile of each potential risk finding. These are sorted by user, with details such as the type of user (PRIVILEGED, SCHEMA, or NON_PRIVILEGED), what roles they hold, the potential risk level assigned to this user, current status of the account, last login, and what schemas they have access to.
9. **TIP**: Click on a user under the **User Name** column for more detail. This shows you all roles and privileges granted to the user and the creation date of the account, which is not shown in the **Critical Potential Risk Details** table. Also note that you can use the **Add Filter** button to narrow down the results. For example you can apply the **Potential Risk** filter if you only want to see users at a specific level of potential risk.
10. Click **View Activity** to review the audit records for the selected user. The All Activity Report displays, with the data pre-filtered for the selected user. You can select other auditing reports from the links on this page.

Note: Your ability to set the scope is determined by the access privileges you have within the tenancy. You can access only compartments and target databases within compartments that you have privileges to access.

View All User Assessments for a Target Database

In the Assessment History, you can view all user assessments for your target databases.

1. From the **User Assessment** page, click the **Target Summary** tab.
2. On the left under **Compartment**, select the compartment that contains the target database for which you want to view the Security Assessment reports. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** if you don't want to include target databases contained in the child compartments.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**.

   The **Assessment Details** page shows you the latest assessment report for your target database.
5. Click **View History**.

   The **Assessment History** page is displayed.
6. From the **Compartment** drop-down list, select the compartment that contains the assessments for the target database. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** if you don't want to include assessments in the child compartments.

The **Assessment History** lists the assessments for your target database.

7. To open and view an assessment, click its name.

   The **Assessment History** page displays the report.

View the User Assessment History for all Target Databases

You can view the user assessments for all target databases in your selected compartment(s) on the Assessment History page

1. Under **Security center**, click **User assessment**.
2. Under **Related resources**, click **Assessment history**.
3. From the **Compartment** drop-down list, select the compartment that contains the assessment that you want to view.
   - Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list assessment located in child compartments.
   - If you select the root compartment and leave **INCLUDE CHILD COMPARTMENTS**, all assessment created in the tenancy are listed.
4. (Optional) Under **Filters**, select a time period from the **Time period** list to narrow the scope of displayed metrics.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. (Optional) To filter by assessment name, under **Filters**, enter an **Assessment name**. Then click **Apply filters**. To reset the filter, erase the entered assessment name. Then click **Apply filters**.
7. View the list of assessment reports in the table.

The table includes the target database name, assessment name (link to the report), whether the assessment is a baseline, when the assessment report was created, the state of the assessment, the number of users in each potential risk category, as well as the number of users with highly privileged roles

> **Note:**
>
> The **Created time** for a baseline will display the date and time when the first baseline was set for any target in the current compartment. It is not necessarily the date and time the target specific baseline you are viewing was created.

> **Tip:**
>
> The baseline assessment may be many rows down in the table. To bring the baseline assessment up to the first row, click the header in the **Baseline** column to re-sort the table.

On this page you can also click **Save Latest Assessment As** to save a copy of the latest assessment under a different name and/or to a different compartment.

View Schema Access Details for a User

User Assessment provides you with the ability to view details about the schemas and tables that a user has access to. You can also see what privileges the user was granted on these schemas and tables. View the **Schema access** column in a User Assessment to find this information.

> **Tip:**
>
> To access the object access related details:
>
> - You will need `read` or `use` permissons on the `data-safe-security-policy-reports` resource. See data-safe-security-policy-reports Resource in the *Administering Oracle Data Safe* guide for more information.
> - You may need to re-run the database privilege script for non-Autonomous Databases. See Grant Roles to the Oracle Data Safe Service on a Non-Autonomous Database in the *Administering Oracle Data Safe* guide for more information.

1. Under **Security center**, click **User assessment**.
2. From the **User Assessment** page, click the **Target summary** tab.
3. (Optional) On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

   > **Note:**
   >
   > The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The User Assessment Details page is displayed, showing you the latest assessment report for your target database.
6. Click on the schemas listed in the **Schema access** column to view more details about the schemas the user has access to.
   This will open a panel on the right.
7. Click on a listed schema in the panel to see the access details at the table level.
   This will bring you to the **Schema details** page. The **Schema details** page includes the following columns:
   - **Table name** - Lists specific tables in the schema or **All tables** if the granted privilege is applicable on all tables in the schema. Click **All tables** to see the list of tables.
   - **Sensitive** - Indicates if the user has access to sensitive data. Data is determined to be sensitive if it is marked as sensitive in a sensitive data model for that target database in Data Discovery.

- **Access Type** - `DELETE`, `INSERT`, `OWNER`, `SELECT`, or `UPDATE`. The table is grouped by this column.
- **Privilege** - The privilege that was granted to the user.
- **Privilege type** - Column Privilege, Object Privilege, Owner Privilege, Schema Privilege on *SCHEMA_NAME*, or System Privilege.
- **Access through object**
  - `TABLE` - Indicates that this privilege is granted directly on the table
  - `VIEW` - Indicates that this privilege is granted on a database view object which is dependent on this table, directly or recursively
- **Grant from role** - Shows the role assigned to the user that provides the listed privileges. Click on this to see the details for the grant path. If there is no value listed, then it is a direct privilege granted to the user.
- **Table privilege grantable** - Indicates what privileges the selected user can grant to other users.
  - `ADMIN_OPTION` - For system privilege, this indicates that the privilege is granted to the user or role with the `ADMIN_OPTION`
  - `GRANT_OPTION` - For column or object privilege, this indicates that the privilege is granted to the user or role with the `GRANT_OPTION`
  - If this is empty it means the user can't grant access to that table to other users
- **Column name** - Lists the column associated with this column privilege.
- **Table access constrained by** - Indicates if the tables of the target database are protected by any of the following security features: Data Redaction, Database Vault, Database view, Oracle Label Security, Real Application Security, SQL Firewall, or Virtual Private Database.
  SQL Firewall is user-based and will show up if there's an eabled SQL Firewall allow-list for this user. SQL Firewall management is only available for Oracle Databaser 23ai target databases.

  If the **Access through object** column is `VIEW`, click to see the **Database view details** report.

8. (Optional) Add basic filters to the report by clicking **+ Add filter**.
9. (Optional) Add advanced filters to the report by clicking **Show advanced SCIM query builder**.

Related Topics

- Advanced Filtering in a Schema Details Report
- Tips for Using the Filter Builder to Create Advanced Filters

Manage User Assessments

User Assessment provides several options for managing security assessment reports. You can refresh and make a copy of the latest assessment. You can also move an assessment, change the name of an assessment, and delete any saved assessment (except the latest assessment).

Refresh the Latest User Assessment

You can refresh the latest user assessment for a target database at any time.

1. From the **User assessment** dashboard, click the **Target summary** tab.
2. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
4. On the **Target summary** tab, locate the line in the table for your target database, and click **View report**. The latest assessment for your target database is displayed. **TIP**: You can click **Add filter** to narrow down the **Assessment details** data. For example,

   ```
   Password
               Changed After Jul 28, 2021 00:00 UTC
   ```

   .
5. At the top of the page, click **Refresh** Now. The **Refresh now** window is displayed.
6. (Optional) In the **Save assessment** box, enter a name for the report.
7. Click **Refresh now**.

   The latest assessment for the target database is updated and saved as the specified name.

You can refresh the latest assessment for a target database at any time.

Save a Copy of the Latest Assessment

You can save a copy of the latest assessment for a target database under a new name and/or in a different compartment.

This feature does not create a new assessment. It only saves a copy of the latest assessment. One use case for this feature may be the need to share the assessment results with other lines of business that do not have access to the assessed target's compartment.

1. Under **Security center**, click **User assessment**.
2. Under **Related resources** on the left, click **Assessment history**.
   The **User assessment history** page is displayed.
3. Select the compartment that contains the assessment. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to not list assessments located in the child compartments.
4. (Optional) Under **Filters**, select a time period from the **Time period** list to narrow the scope of displayed metrics.
5. (Optional) Under **Filters**, select a target database from the **Target databases**, list to narrow the scope of displayed metrics.
6. Click **Save latest assessment as**.
   The **Save latest assessment** window is displayed.
7. From the **Target database** drop-down list, select the name of your target database.

8. In the **Assessment name** box, enter a name for the new copy of the assessment.
9. (Optional) In the **Saved assessment description** box, describe the assessment.
10. From the **Saved assessment compartment** drop-down list, select the compartment to which you want to save the assessment.
11. Click **Save latest assessment**.

Move a User Assessment

You can move a user assessment to another compartment, provided the assessment is not the latest assessment for a target database, nor an assessment that is on a daily schedule. Saved assessments that you can move are listed on the Assessment History page.

1. On the **User assessment** page, under **Related resources** on the lower left, click **Assessment History**.
2. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a time period from the **Time period** list to narrow the scope of displayed metrics.
4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
5. On the **Assessment history** page under **Assessment Name**, click the assessment that you want to move to another compartment.
   The report is displayed.
6. From the **More actions** menu, select **Move resource**.
   The **Move resource** dialog box is displayed.
7. Select the new compartment and then click **Move resource**.

You cannot move the latest assessment. However, if the target database is moved to a different compartment, then the next time the latest assessment runs, the latest assessment automatically moves to the same compartment as the target database. This happens whether the latest assessment is a started by a scheduled run or by clicking **Refresh now.**

Change the Name of a User Assessment

On the Assessment Information tab you can change the auto-generated name of the assessment to a name that has specific meaning for your organization. You and other users can then more easily identify assessments. For example, you could change the name of the auto-generated security assessment `UA_1631303036184` to `UA_main_compart4_targdb15a`. It is advisable to include a segment that indicates the assessment is a user assessment, such as the `UA_` prefix in the auto-generated assessment name.

1. From the **User Assessment** page, click the **Target Summary** tab.
2. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.

4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The **User Assessment Details** page is displayed, showing you the latest assessment report for your target database
5. Click the **Assessment Information** tab to view details about the assessment.
6. At the **Name** field (first field at the top) click the pencil icon. Change the name and then click the save icon.

   The page may take a few moments to process the change and display the update. When the status under the large UA icon is `SUCCEEDED`, you should see the new name.

Delete a User Assessment

You can delete any user assessment of a target database, except for the latest assessment.

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources** on the left, click **Assessment History**.
3. On the left under **Compartment**, select the compartment that contains the target database(s) for which you want to view the Security Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.
4. (Optional) Under **Filters**, select a time period from the **Time period** list to narrow the scope of displayed metrics.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. Click the name of the assessment report that you want to delete.
   The report is displayed.
7. From the **More Actions** menu, select **Delete**.
   The **Confirm** dialog box is displayed asking you to confirm the deletion.
8. Click **Delete** to confirm.

Advanced Filtering in a Schema Details Report

Advanced filtering of schema details can provide flexibility in the way that data is analyzed and reviewed, by allowing organizations to specify complex conditions and multiple criteria that must be met in order for data to be included or excluded from the analysis.

To apply advanced filters in the report, do the following:

1. View a **Schema details** report. For more information see View Access Details for a Database User.
2. Click **Show Advanced SCIM Query Builder**.
3. Use the provided filter builder and dropdowns to type in your filter(s). Advanced filtering uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:
   - `co`: matches resources with an attribute that contains a given string
   - `eq`: matches resources with an attribute that is equal to a given value (not case sensitive)
   - `eq_cs`: matches resources with an attribute that is equal to a given value (case sensitive)

- `ew`: matches resources with an attribute that ends with a given string
- `ge`: matches resources with an attribute that is greater than or equal to a given value
- `gt`: matches resources with an attribute that is greater than a given value
- `in`: matches resources with an attribute that is equal to any of given values in list
- `le`: matches resources with an attribute that is less than or equal to a given value
- `lt`: matches resources with an attribute that is less than a given value
- `ne`: matches resources with an attribute that is not equal to a given value
- `not_in` : matches resources with an attribute that is not equal to any of given values in list
- `pr`: matches resources with an attribute if it has a given value
- `sw`: matches resources with an attribute that starts with a given string

Operators can be grouped using parentheses to specify the order.

Filters can also be combined using logical operators such as `and` and `or`.

> **Note:**
>
> If you have any basic filters currently applied they will appear in the query builder as well.

4. Click **Apply**.

To clear the query builder, click **Clear**. This will clear any basic filters applied as well.

Tips for Using the Filter Builder to Create Advanced Filters

- Pressing the escape key while in advanced filtering mode will clear the whole query.
- Pressing the space key will display the drop down with the list of available attributes or operators.
- Pressing the space key after entering a value like `tablename (employee_list)` will enclose the string with quotes: `("employee_list")`
- Pressing enter will close the drop down listing the operators and attribute names.
- If a value like Privilege type has spaces in it, typing space will enclose the first word within quotes, `"Object" Privilege`. You will have to move the cursor back to the enclosed string and continue typing the rest of the string value.
- If you build a filter in advanced filtering that can't be displayed in basic filters, you can't switch back to basic filtering mode. For example, advanced filters with the or condition can't be displayed in basic filtering.
- A custom report with basic filter can be updated with advanced filter and saved.

For more information about SCIM, see the protocol documentation at https://www.rfceditor.org/rfc/rfc7644.

For more information about filtering in SCIM, see the filtering section of the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644#section-3.4.2.2.

Schedule User Assessments

User Assessment has two schedule types: LATEST and SAVED.

There is a default schedule that controls when the latest assessment for your target runs (referred to as `LATEST` schedule). You can rename or update this schedule. You cannot delete it.

Additionally, you can create a custom schedule (referred to as a `SAVED` schedule) to periodically save a copy of the latest assessment for your target database. You can rename, update, or delete `SAVED` schedules.

> **Important:**
>
> When you create or modify schedules, enter all schedule times in UTC (Coordinated Universal Time). Base your schedules on the UTC offset for the region where your tenancy is hosted.

Schedule to Save the Latest User Assessment

You can create a schedule to periodically save a copy of the latest user assessment for your target database to a compartment of your choice.

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. Click **Add Schedule**.
   The **Add Schedule** window is displayed.
4. In the **Schedule Name** box, enter a name for the schedule.
5. From the **Schedule Compartment** drop-down list, select the compartment to which you want to save the schedule.
6. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
7. If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
8. If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
9. In the **Time** box, enter a time in the `hh:mm aa` format. Alternatively, click the **Time** box and select a time from the drop-down list.
10. From the **Target Database** drop-down list, select the target database for which you want to create the schedule.
11. Click **Add Schedule**.
    The **Schedule Details** page is displayed. The schedule is created when the status reads `SUCCEEDED`.

Each time a copy of the latest assessment is saved, the copy is listed in the Assessment History.

Update a User Assessment Schedule

You can update a user assessment schedule from two locations in Oracle Data Safe. One location is from the Schedule Details page and the other is from the User Assessment Details page. Select the appropriate tab below to see the steps for updating a schedule from your desired location.

From the Schedule Details Page

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

   > **Note:**
   >
   > The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Update Schedule**.
   The **Update Schedule** window is displayed.
8. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
   - If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
   - If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
9. In the **Time** box, enter a UTC time in the format `hh:mm ss`. Alternatively, click the **Time** box and select a time from the drop-down list.
10. Click **Update Schedule**.

The schedule is updated when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. Under **Security Center**, click **User Assessment**.
2. From the **User Assessment** page, click the **Target Summary** tab.

3. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The User Assessment Details page is displayed, showing you the latest assessment report for your target database.
6. Click the **Assessment Information** tab to view details about the assessment.
7. Click **Update Schedule**.
   The **Update Schedule** window is displayed.
8. From the **Schedule Type** drop-down list, select **Daily**, **Weekly**, or **Monthly**.
   - If you selected **Weekly** as the schedule type, in the **Every** drop-down list, select a week day.
   - If you selected **Monthly** as the schedule type, in the **Day** drop-down list, select the day number.
9. In the **Time** box, enter a UTC time in the format `hh:mm ss`. Alternatively, click the **Time** box and select a time from the drop-down list.
10. Click **Update Schedule**.

The schedule is updated when the status shown on the page is `SUCCEEDED`.

Stop a User Assessment Schedule

- From the Schedule Details page
- From the Assessment Details page

From the Schedule Details page

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Stop schedule**.
8. Click **Yes** in the confirmation dialog.

The schedule is stopped when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. Under **Security Center**, click **User Assessment**.
2. From the **User Assessment** page, click the **Target Summary** tab.
3. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The User Assessment Details page is displayed, showing you the latest assessment report for your target database.
6. Click the **Assessment Information** tab to view details about the assessment.
7. Click **Stop schedule**.
8. Click **Yes** in the confirmation dialog.

The schedule is stopped when the status shown on the page is `SUCCEEDED`.

Start a Previously Stopped User Assessment Schedule

From the Schedule Details page

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains your schedule. Optionally deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments of the selected compartment.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. In the table listing all of the schedules, click the name of your schedule.
   The **Schedule Details** page is displayed.
7. Click **Start schedule**.
   The target database will get assessed again periodically according to the same schedule that was previously defined, by default this is weekly. If you would like to update the schedule see, Update a User Assessment Schedule.

The schedule is started when the status shown on the page is `SUCCEEDED`.

From the Assessment Details page

1. Under **Security Center**, click **User Assessment**.
2. From the **User Assessment** page, click the **Target Summary** tab.
3. On the left under **List Scope**, select the compartment that contains the target database(s) for which you want to view the User Assessment reports. Select the **INCLUDE CHILD COMPARTMENTS** check box if you also want to be able to view reports for target databases that reside in child compartments too.

> **Note:**
>
> The schedule that generates the latest assessment for a target database is available in the same compartment as the target database.

4. On the **Target Summary** tab, locate the line in the table for your target database, and click **View Report**. The User Assessment Details page is displayed, showing you the latest assessment report for your target database.
5. Click the **Assessment Information** tab to view details about the assessment.
6. Click **Start schedule**.
   The target database will get assessed again periodically according to the same schedule that was previously defined, by default this is weekly. If you would like to update the schedule see, Update a User Assessment Schedule.

The schedule is started when the status shown on the page is `SUCCEEDED`.

Delete a User Assessment Schedule

You can delete any schedule from the Schedule Details page, except for the schedule that generated the latest assessment for a target database.

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **Schedules**.
   The **Schedules** page is displayed.
3. From the **Compartment** drop-down list, select the compartment that contains the schedule that you want to delete. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to filter out schedules that reside in the child compartments.
4. (Optional) Under **Filters**, select a **Schedule type** from the drop-down list.
5. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
6. In the table listing all of the schedules, click the name of the schedule that you want to delete.
   The **Schedule Details** page is displayed.
7. Click **Delete**.
   A Confirm dialog box is displayed asking you to confirm the deletion.
8. Click **Delete** to confirm.

The schedule is permanently deleted.

Compare User Assessments

In User Assessment, you can compare two assessment for a target database to determine if there has been any security drift in the time interval between the two assessments.

Compare options are only visible when you are viewing the latest assessment.

Overview: Comparing User Assessments

It is important to be able to track how the potential user risks in a target database change over time so that you have the data you need to maintain the optimal security posture and to observe trends and patterns in changes that affect security. This is done by comparing User Assessments of the target database from two points in time, which shows you the security drift between two selected assessments.

There are two comparison options available in Oracle Data Safe:

- **Compare With Baseline**

  Compare a saved User Assessment against a baseline User Assessment of the same target database. This requires that you set a User Assessment that reports a relatively low level of potential risk as the baseline, or starting point, and then you can compare the Latest Assessment against it.

- **Compare Assessments**

  Compare a previously-saved User Assessment against the latest User Assessment of the same target database.

> **Note:**
>
> The comparison operations require read permission on the `data-safe-work-requests` resource in IAM.

Compare With Baseline

When an assessment indicates that the level of potential risk from user accounts on a target database is low, consider setting that assessment as the baseline. You can then compare the Latest Assessment of the same target database against the baseline.

For example, suppose that for one target database you have schedule assessments on a monthly cycle and the assessment run on March 1 reveals a number of potential user risks. You address the most significant ones during that month and then find that April 1 assessment looks much cleaner, giving you confidence that the security posture is now strong. You may then want to set the April 1 assessment as the baseline. If a baseline is set, then for each scheduled assessment, Oracle Data Safe automatically reports new potential risks as deviations from the baseline (security drift).

However, you do not have to wait for the next scheduled assessment to get comparison data. Once you have set a baseline you can manually run **Compare With Baseline** to check the Latest Assessment for any security drift from the baseline.

Compare Assessments

In addition to **Compare With Baseline**, another comparison of interest is how the current security posture compares with the security posture from some point in the past. This comparison does not require a baseline. You can run **Compare Assessments** to compare the Latest Assessment against any previously-saved assessment.

Structure of a User Assessment Comparison

Both Compare With Baseline and Compare Assessments provide a table that lists each user account where there as been some change that may impact the security posture of the selected target database. In the case of Compare With Baseline, these are deviations from the baseline that appear in the latest assessment of the target database. In the case of Compare Assessments the deltas reported are between the selected saved assessment and the latest assessment. The table is sorted by **Potential Risk**.

For each User Name. the Status column indicates if this is a new, existing, or deleted user. In case of Compare With Baseline, the status is relative to the baseline. A new user is one that did not exist when the baseline assessment ran. A deleted user is one that did exist in the baseline but does not exist in the latest assessment. An existing user is one where the account was modified after the run of the assessment that has been set as the baseline.

In the case of Compare Assessment, a new user is one that exists latest assessment, but did not exist in the earlier assessment. Likewise, a deleted user no longer exists in the latest assessment. An existing user is one found in both compared assessments and whose account has been modified.

The Comparison Results column shows whether something was added, removed, or modified and names the areas (called `User Details` in User Assessment) where changes have occurred.

Get the Comparison Details

For any **User Name** listed, click on **Open Details** in the Comparison Results column. The Comparison Details page provides the name and assessment data of the baseline and the latest assessment that are being compared. And shows the specific changes that appear in the latest assessment, relative to the baseline. For example, in this case the account HR existed in the baseline and the latest assessment indicates that it was modified at some point prior to the latest assessment. You can see that a number of grants have been modified and one new grant was added.

Set the Latest User Assessment or a Saved Assessment as the Baseline for a Target Database

You can set an assessment for a target database as a baseline.

> **Note:**
>
> The **Set as Baseline** operation requires `read` permission on the `data-safe-work-requests` resource in IAM.

1. Under **Security Center**, click **User Assessment**.
2. From the **User Assessment** page, click the **Target Summary** tab.
3. From under **List Scope**, select the compartment that contains your target database.
4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. In the **Target Summary** table, locate your target database and then click the **View Report** link to open the latest assessment report.
   The **User Assessment Details** page shows the latest assessment.
6. Review the user accounts, their privileges, and potential risk level.
7. If you are confident that the overall potential risk level reported in the latest assessment is acceptable in the baseline, then click **Set as Baseline** and then click **Yes** to confirm.

If instead you want to set an earlier assessment as the baseline, then back on the same **User Assessment Details** page where the latest assessment is displayed, click **View History**.

1. On the **Assessment History** page, find an assessment that looks like a potential candidate for use as the baseline. At this level you can see how many roles are granted within the target database and how many accounts are high or critical potential risk.
2. In the **Assessment Name** column, click on the assessment to see more details. Here you can see all privileged and non-privileged users as well as the open potential risks posed by each user.
3. If you are confident that this assessment is a good choice for the baseline, then click **Set as Baseline**.
   The **Set as Baseline** dialog box is displayed.

4. Click **Yes** to confirm.

Once you have set a baseline, future assessments of the target database automatically include a check for security drift, which is any deviation from the baseline. You are also then able to manually compare any saved assessment with the baseline to check for security drift.

Compare the Latest User Assessment with the Baseline

If you have set a baseline User Assessment for the selected target database, you can compare the latest assessment of the same target database with the baseline. To do this, open the latest assessment report and use the **Compare with Baseline** feature. This comparison shows you what user accounts have been added, deleted, or modified in the interval between the baseline and the latest assessment. In the case of modified users, the comparison shows the details of the modifications.

1. Under **Security Center**, click **User Assessment**.
2. Click the **Target Summary** tab.
3. From the **Compartment** drop-down list, select the compartment that contains your target database. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list target databases in the child compartments.
4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. Open the latest assessment report. To do this, in the **Target Summary** table, locate the line for your target database, and click **View Report** in the **Last Assessed On** column. The **Assessment Details** page is displayed, showing you the latest assessment for the target database. On the left under **Resources**, there are two options to compare assessments: **Compare with Baseline** and **Compare Assessments**.
6. Click **Compare With Baseline**.
   A **Comparison With Baseline** section is added to **Assessment Details** page.
7. To do a comparison, click **Compare Now**.
   The Comparison report is displayed.

The comparison shows what has changed in the latest assessment, relative to the baseline. The **Status** column shows whether a user is:

- `New` – did not exist in the baseline.
- `Deleted` – existed in the baseline, but does not exist in the Latest Assessment.
- `Existing` – present in both assessments but has been modified in the interval between the baseline and the latest assessment.

The **Comparison Results** column shows whether something in the user account was added, removed, or modified and names the areas (called `User Details` in User Assessment) where changes have occurred.

> **Note:**
>
> The comparison shows the deltas between the two assessments. User accounts that exist in both assessments, but have not been modified are not listed.

Compare the Latest Assessment With a Saved Assessment

You can compare the Latest Assessment with an earlier assessment to check for security drift.

1. Under **Security Center**, click **User Assessment**.
2. Click the **Target Summary** tab.
3. From the **Compartment** drop-down list, select the compartment that contains your target database. Optionally, deselect **INCLUDE CHILD COMPARTMENTS** to not list target databases in the child compartments.
4. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics and charts.
5. To view the latest assessment for your target database, in **Target Summary** locate the row for your target database. Click **View Report** in the **Last Assessed On** column.
   The **User Assessment Details** page is displayed, showing you the latest assessment for the target database.
6. Under **Resources** on the left, click **Compare Assessments**.
   The **User Assessment Details** page updates to include a **Compare With Other Assessments** section.

   Note: If the assessment report that you want to select is located in a different compartment than the one that is shown, click **Change Compartment**, and select a different compartment.
7. From the **Select Assessment** drop-down list, select the assessment that you want to compare with the latest assessment.
8. Click **Compare Now**.

The comparison shows what has changed in the latest assessment, relative to the earlier assessment that you selected. The Status column shows whether a user is:

- New – did not exist in the earlier assessment.
- Deleted – existed in the earlier assessment but does not exist in the latest assessment.
- Existing – present in both assessments but has been modified in the interval between the earlier assessment and the latest assessment.

The Comparison Results column shows whether something in the user account was added, removed, or modified and names the areas (called User Details in User Assessment) where changes have occurred.

NOTE: The comparison shows the deltas between the two assessments. User accounts that exist in both assessments, but have not been modified are not listed.

For any User Name listed, click on **Open Details** in the Comparison Results column. The Comparison Details page provides the name and assessment data of the baseline and the latest assessment that are being compared. And shows the specific changes that appear in the latest assessment, relative to the baseline. For example, in this case, the account HR existed in the baseline and the latest assessment. The comparison indicates that it was modified at some point prior to the latest assessment. You can see that a number of grants have been modified and one new grant was added.

Generate and Download a PDF or XLS Report of a User Assessment

You can generate and download a PDF or XLS-formatted report based on the latest or baseline assessment for a target database.

1. View the latest or baseline assessment for a target database.
2. From the **More Actions** menu, select **Generate Report**.
   The **Generate Report** dialog box is displayed.
3. Select the report format that you want to use. You can choose either PDF or XLS.
4. Click **Generate Report**.
5. Wait for the report to complete, then click **Close**.
6. You can then pull down **More Actions** again and click **Download Report**.
7. Save the report to your local computer.

> **Note:**
>
> There is no option to generate a report from an assessment other than the latest or baseline assessment.

User Profiles

With User Profiles, you gain a comprehensive understanding of the password-related attributes associated with your Oracle Database user profiles. User Profiles enables you to identify and address any weak login and password governance policies, helping to strengthen the system's overall security.

About User Profiles

As part of User Assessment, User Profiles allow you to view password-related attributes associated with your database users via user profiles. After identifying potential misconfigurations or discrepancies between user profiles in different databases, you can implement best practices such as enforcing strong, complex passwords and limiting the number of failed login attempts to strengthen the system's overall security.

A user profile is a collection of password-related attributes determining the rules and restrictions for logging in and managing passwords within a database. The database can contain multiple user profiles, each associated with zero to many users. Each user in an Oracle database is assigned to a single user profile at any given time. If a user is not explicitly assigned to a profile, they will be automatically assigned to the DEFAULT profile.

As a best practice and to ensure proper security and governance of your users' logins and passwords, it's recommended to customize the DEFAULT profile to fit your specific policies and requirements. This way, all users who aren't created with a defined user profile will still be governed by your organization's standards. Additionally, creating specific user profiles tailored to particular users or application needs would be best. For instance, you should allow more failed login attempts, such as five, for interactive user accounts, as users may make mistakes entering their passwords. It's also advisable to automatically unlock locked accounts after

some inactivity. This will block automated brute-force attacks from succeeding while not preventing interactive users from retrying their password to log in after some time. However, for service accounts, limit the number of failed login attempts to a lower value, like two, as these accounts are less likely to fail due to incorrect passwords.

Regardless of the user profile, setting a password verification function is essential to ensure all passwords meet complexity standards. By taking these steps, you can enhance the security of your system and protect your users' sensitive information.

> **Note:**
>
> While a user profile comprises of password and resource-related attributes, Data Safe focuses solely on password-related attributes.

Password parameters include:

FAILED_LOGIN_ATTEMPTS	Maximum times the user is allowed in failed login before locking the user account
PASSWORD_LIFE_TIME	Number of days the password is valid before the expiry
PASSWORD_REUSE_TIME	Number of days after the user can use the already-used password
PASSWORD_REUSE_MAX	Number of times the user can use the already-used password
PASSWORD_LOCK_TIME	Number of days the user account remains locked after failed login
PASSWORD_GRACE_TIME	Number of grace days for the user to change the password
PASSWORD_VERIFY_FUNCTION	PL/SQL that can be used for password verification
SEC_CASE_SENSITIVE_LOGON	To control the case sensitivity in passwords
PASSWORD_ROLLOVER_TIME	The number of days the password rollover is allowed. The minimum value can be 1/24 day (1 hour) to 60 days.

Oracle Data Safe uses the user profiles that are already defined on the target database. User Profiles in Data Safe does not allow you to create or edit user profiles, they can only be viewed or analyzed. Possible analysis includes:

- How many users are assigned to the DEFAULT profile, other Oracle-provided profiles, or your custom profiles in your databases or fleet.
- How many databases have a specific named user profile so you can identify loosely defined profiles and discrepancies, harden them, and work towards consistency across all your databases to reduce risk.
- For each target database, what are the all the password-related attributes for each profile, including the password verification function code.

To create or edit user profiles in your target database see the information in the Oracle Database SQL Language Reference guide.

View User Profiles

User Profiles shows two charts displaying the distribution of users by profile and users with password complexity.

The **User Profile Summary** tab shows a table of profiles, how many databases have each profile, and how many total users are in each profile across all databases. The profiles are aggregated by name, even though profiles of the same name might have different parameters in different target databases. To view the parameters of the user profile in each target databases, see View User Profile Details.

The **Target Summary** tab show a table of all profiles in target databases and specific password parameters for each one, including the number of allowed failed logins, the password verification function that checks for password complexity (if any), how many sessions a user can have open, if the profile is user-created, and the number of users on that profile. To view the user details and password parameters of a user profile, see View User Profile Details by Target.

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **User Profiles**.
   The User Profiles page is displayed.
3. (Optional) Narrow the scope of the User Profile and Target Summary tabs by using **List Scope**.
   a. Select a compartment you have access to from the **Compartment** list.
   b. Select or deselect **Include child compartments**.
4. (Optional) Narrow the scope of the Target Summary tab by using **Filters**.
   a. Select a target database from the **Target Database** list.
   b. Select a profile name from the **Profile Name** list.
   c. Select a set of password requirements from the **Password Requirements** list.

View User Profile Details

The User Profile Details show the total number of target databases and users that have the selected user profile.

In addition, the table lists the target databases that have the selected user profile, the number of users in that profile per target database, the parameters that control the number of allowed failed login attempts, the password verification function that enforces password requirements, the permitted inactivity period set, the account lockout period, and sessions per user.

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **User Profiles**.
3. Select one of the user profiles from the list in the **User Profile Summary** tab.
   The details of the selected user profiles are displayed.
4. (Optional) Add a filter using **Add Filter**.
   a. Select a type from the drop down list.
   b. Select an operation from the drop down list.
   c. Type in a value.
   d. Click **Apply**.
   e. Repeat the above steps to apply more filters.
5. (Optional) Click **Manage Columns** to select and deselect columns to be displayed. Click **Save Changes.**

View User Profile Details by Target

The User Profile Details by Target shows the profile details in that specific target database. It lists the user assessment OCID, the compartment, the specifics of the password parameters, and how many users in the target database have been assigned the selected profile.

The password requirements field lists the password verification that is used to enforce password complexity checks and by clicking **View Details** a user can see the details of the function (PL/SQL) code.

In addition, the table lists the details of the users in the specified profile. This includes the user name, the user type, the potential risk level, their status, their last login, and a link to a filtered report of all operations performed by the selected user.

Accessing User Profile Details by Target from the Target Summary Tab

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **User Profiles**.
3. Select one of the user profiles from the list in the **Target Summary** tab.
   The details of the selected user profile are displayed.
4. (Optional) Add a filter using **Add Filter**.
   a. Select a type from the drop down list.
   b. Select an operation from the drop down list.
   c. Type in a value.
   d. Click **Apply**.
   e. Repeat the above steps to apply more filters.
5. (Optional) Click **Manage Columns** to select and deselect columns to be displayed. Click **Save Changes.**

Accessing User Profiles Details by Target from the User Profile Summary Tab

1. Under **Security Center**, click **User Assessment**.
2. Under **Related Resources**, click **User Profiles**.
3. Select one of the user profiles from the list in the **User Profile Summary** tab.
   The details of the selected user profile are displayed for all targets where this profile is available.
4. Select one of the targets where the profile is available from the list in the **User Profiles** table.
   The details of the selected user profile are displayed.
5. (Optional) Add a filter using **Add Filter**.
   a. Select a type from the drop down list.
   b. Select an operation from the drop down list.
   c. Type in a value.
   d. Click **Apply**.
   e. Repeat the above steps to apply more filters.

6. (Optional) Click **Manage Columns** to select and deselect columns to be displayed. Click **Save Changes.**

Create and Modify Event Notifications in User Assessment

You can create and modify event notifications in User Assessment.

Creating Event Notifications for User Assessment

In Data Safe you can create event notifications for User Assessment related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **User assessment**.
2. Click the **Notifications** tab.
3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See User Assessment Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
12. Click **Create notification**.

Modifying Event Notifications For User Assessment

After creating event notifications in User Assessment in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **User assessment**.
2. Click the **Notifications** tab.
3. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **User assessment**.
2. Click the **Notifications** tab.
3. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

4

Activity Auditing

This section discusses how to configure audit data collection in Oracle Data Safe by using the Activity Auditing feature.

Activity Auditing Overview

Activity Auditing lets you collect audit data from your target databases so that you can monitor database activities.

About Activity Auditing

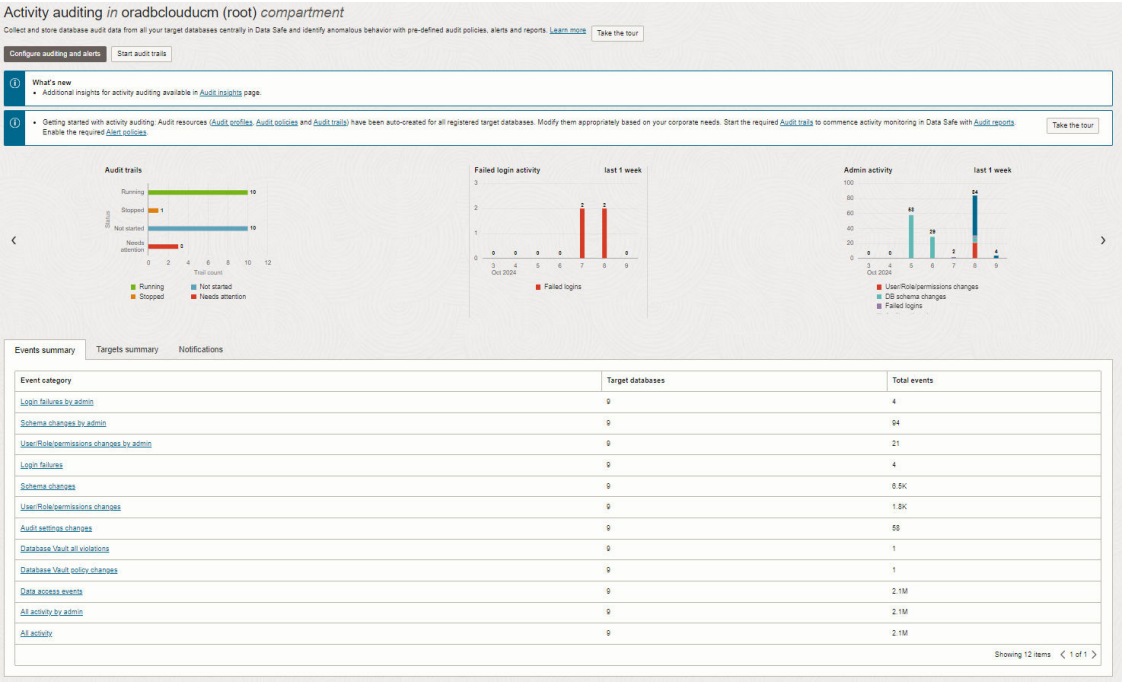
You entrust your databases to your database administrators, account owners, and end users. However, it's important to monitor database activity regularly because accounts are always at risk for being compromised or misused. Activity Auditing in Oracle Data Safe helps to ensure accountability and improve regulatory compliance.

With Activity Auditing, you can collect and retain audit records per industry and regulatory compliance requirements and monitor user activities on Oracle databases. For example, you can audit access to sensitive data, security-relevant events, administrator and user activities, activities recommended by compliance regulations like the Center for Internet Security (CIS), and activities defined by your own organization. You can collect up to one million audit records per month per target database in Oracle Data Safe for free.

Activity Auditing Dashboard

By default, the Activity Auditing dashboard shows you a summary of audit events for the last one week for all target databases, in the form of charts and tables. This gives you a broad overview of audit events across all target databases monitored by Oracle Data Safe. You can modify the filters set on target database and time period as needed. The charts and tables are immediately updated.

Figure 4-1 Activity Auditing Dashboard



The **Failed login activity** chart shows you the number of failed logins on all or selected target databases for the specified time period.

The **Admin activity** chart shows you the number of database schema changes, logins, audit setting changes, and entitlement changes on all or selected target databases for the specified time period.

The **All activity** chart shows you the total count of audit events on all or selected target databases for the specified time period.

The **Events summary** tab lists the following audit event categories. For each category, you can view the number of target databases that have an audit event in each event category as well as the total number of events per category.

- Login failures by admin
- Schema changes by admin
- Entitlement changes by admin
- Login failures
- Schema changes
- Entitlement changes
- Audit settings changes
- Database Vault all violations
- Database Vault policy changes
- Data access events
- All activity by admin
- All activity

The **Targets summary** tab shows you various audit event counts per target database. Audit events include the number of login failures, schema changes, entitlement changes, audit settings changes, all activity (all audit events), database vault realm violations and command rule violations, and database vault policy changes. If there are no audit events for a target database, the target database isn't listed.

The **Notifications** tab shows you what event notifications and subscriptions you have created for Activity auditing. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show Events that you have created directly within Data Safe. In addition to displaying existing event notifications, you can also create new notifications by using the **Create notification** button. See Create and Modify Event Notifications in Activity Auditing for more information.

Audit Profiles, Audit Policies, Audit Trails, and Archive Data Retrievals

Activity Auditing resources that pertain to audit data collection, retention, and retrieval are audit profiles, audit policies, audit trails, and archive data retrievals.

An **audit profile** resource gives you the flexibility to compute how much audit data is available on the target database for each audit trail that Oracle Data Safe has not yet collected. This helps you evaluate the initial audit data volume when you configure collection in Oracle Data Safe. You also can compute how much audit data Oracle Data Safe has already collected from the target database.

An **audit profile** defines the online retention period, offline retention period, and the paid usage settings for a target database.

An **audit policy** resource represents the audit policies for the target database, their corresponding provisioning status, and which policies are enabled or disabled on the target database.

An **audit trail** represents audit record collection from the target's database trail such as UNIFIED_AUDIT_TRAIL, which provides documentary evidence of the sequence of activities. Configuring audit trails in Oracle Data Safe, and enabling audit data collection on the audit trails copies the audit records from the target database's audit trail into the Oracle Data Safe repository.

An **archive data retrieval** represents an archive retrieve request for audit data. You can retrieve audit data for a target database from the archive and store it online.

Activity Auditing Reports

Oracle Data Safe generates several predefined audit reports that you can view from the **Audit Reports** page. The reports track general database activities, such as audited SQL statements, application access activities, and user login activities, as well as Oracle Data Safe activities.

The following table describes each report.

Report Name	Description
All Activity	All audited activities
Admin Activity	Report tracking database activities on admin users as identified in the User Assessment feature. Please note that changes on users may not be reflected immediately in the report and might take up to 12 hours to appear.
User/Entitlement Changes	User creation/deletion/privilege and role changes

Report Name	Description
Audit Policy Changes	All changes in audit policies
Login Activity	Database login attempts
Data Access	Database query operations
Data Modification	Data modification activities (DMLs)
Database Schema Changes	Database schema changes (DDLs)
Data Safe Activity	Activity generated by the Oracle Data Safe service
Database Vault Activity	Auditable activities of enabled Oracle Database Vault policies in target databases, including mandatory Database Vault configuration changes, realm violations, and command rule violations
Common User Activity	Report tracking database activities on common users as identified in the User Assessment feature.
Database Error	Report tracking errors reported in database for activities that are audited.
Data Extraction Activity	Report tracking DataPump and RMAN activities in database.
Sensitive Data Activity	Report tracking database activities on sensitive objects as identified in the sensitive data models of the Data Discovery feature.

> **Note:**
>
> This report will only display data if there is a Sensitive Data Model for the target database.

SQL Firewall audited violations	Report tracking all SQL Firewall violations that are audited in the database.

Prerequisites for Using Activity Auditing

These are the prerequisites for using Activity Auditing:

- **Register the target databases that you want to use with Activity Auditing.**
- **Grant the Audit Collection and Audit Setting roles on the target database.** A Database Administrator can grant these roles to the Oracle Data Safe Service Account on the target database.
- **Obtain permission in Oracle Cloud Infrastructure Identity and Access Management (IAM) to use the Activity Auditing feature in Oracle Data Safe.** An OCI administrator can grant `view` or `manage` permission as needed on the following resources:
  - `data-safe-work-requests`
  - `data-safe-audit-profiles`
  - `data-safe-audit-trails`
  - `data-safe-audit-events`
  - `data-safe-archive-retrievals`
  - `data-safe-report-definitions`

- `data-safe-reports`
- `data-safe-audit-policies`

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-audit-family` in the relevant compartments, which would include permissions on all of the resources above. See data-safe-audit-family Resource in the *Administering Oracle Data Safe* guide for more information.

> **See Also:**
>
> The *Administering Oracle Data Safe* guide provides these sections to help with establishing the prerequisites:
>
> - Grant Roles to the Oracle Data Safe Service Account on Your Target Database describes the roles required for Activity Auditing and for other Oracle Data Safe features.
> - OCI Resources for Oracle Data Safe describes the permissions for each resource in Oracle Data Safe.

Activity Auditing Workflow

The general steps for collecting and managing audit data for a target database are as follows:

1. Register your target database. Oracle Data Safe creates an audit profile, creates an audit policy, and discovers the audit trails on your target database.
2. Review and modify the audit profile to customize audit data retention settings and paid usage settings.
   - Specify if you want to collect audit data for your target database after it reaches the monthly free limit.
   - Specify the number of months that you want to retain audit data online and archive audit data.
3. Provision audit policies for your target database.
   - Select predefined Oracle Data Safe audit policies, predefined Oracle Database audit policies, individual custom policies, and audit compliance standards policies to provision on your target database.
   - For some audit policies, specify users to audit or exclude users from auditing.
   - Retrieve updates to existing audit policies.
   - Retrieve new audit policies that are created on your target database post target database registration.
4. Discover additional audit trails, remove audit trails, and enable auto purge on your target database as needed.
5. Start collecting audit data by starting the audit trail(s) for your target database.
6. Monitor and analyze the audit data on the Activity Auditing dashboard and in audit reports.
7. Set up event notifications. For example, you can subscribe to the `Audit Trail Collection Free Limit Warning` event to be automatically informed if an audit collection reaches 80% of the free limit.

8. Manage audit data collection by adjusting audit trails.
   - Start, stop, and resume collecting audit data as needed.
   - Enable or disable auto purge.
   - Discover new audit trails.
   - Delete unused audit trails.
9. Retrieve archived audit data when needed.
   - You can retrieve audit data from the Oracle Data Safe archive if you have previously archived audit data for your target database.
10. View and Manage Audit Reports.
    - You can view and schedule audit reports, set filters and modify columns in audit reports, download audit reports as PDF, XLS, or JSON files, as well as create, update, and delete custom audit reports.
11. Configure Auditing and Alerts.
    - You can configure auditing and alerts or start auditing trails by using the wizard in Activity Auditing.

Audit Insights

Audit Insights provides more detailed information about auditing data including the targets, objects, schemas, and users that produce the most activity.

About Audit Insights

Audit Insights provides you with a more detailed overview of auditing data for your target databases over a specified amount of time. You can use the various key metrics and charts to examine your activity auditing and refine your auditing policies.

Audit Insights compiles information from Activity Auditing to provide you with key metrics and summarized views. Analyzing your top items by audit volume can help you identify what audit policies should be adjusted to improve the overall security of your target databases.

Typical use cases include:

- Identifying the top database(s) from the fleet of monitored targets contributing the most to the audit volume.
- Identifying the audit policies generating the most audit volume across the fleet.
- Identifying the client connections generating the most audit volume across the fleet.
- Identifying if your audit policies are capturing enough database activity on your intended schemas and objects.
- Identifying if your audit policies are enabled on the right set of database users whose activity you want to monitor.
- Identifying if any of the databases in your fleet are generating a large audit volume unintentionally or are not generating enough audit volume to meet security requirements.
- Analyzing audit volume by different filters including time-period and target scope.

Audit Insights provides you with key metrics such as the total number of:

- Targets

- Database users
- Client hosts
- Data definition language (DDL) commands
- User and entitlement changes
- Data manipulation language (DML) commands
- Login failures
- Events

The Audit Insights charts summarize the percentage breakdown by audit volume for each of the following items:

- Targets
- Audit policies
- Schemas
- Objects
- Database users
- Client hosts

Clicking a section of any chart will display an All Activity report with filters applied based on the selected chart section.

View Audit Insights

1. Under **Security Center**, click **Activity Auditing**
2. Under **Related Resources**, click **Audit Insights**
   The Audit Insights page displays key metrics and charts summarizing the percentage that the top ten individual resources make up of the audit volume of the top ten resources of a resource type.

   Each chart provides a legend for the resources included in the chart. At the end of each resource name is the target database that this resource is associated with. This can be seen by hovering over the resource name if not immediately visible.
3. (Optional) Deselect one or more individual resources from the legend of each chart to analyze the remaining resources by audit volume.
4. (Optional) Under **List Scope** select a compartment from the **Compartment** list.
   The selected compartment will be displayed in the sub-title of the page.
5. (Optional) Under **List Scope** select or deselect to include child compartments.
6. (Optional) Under **Filters** select a time period from the **Time Period** list to narrow the scope of displayed metrics and charts.
   The selected time period will be displayed in the sub-title of the page.
7. (Optional) Under **Filters** select a target database from the **Target Databases** list to narrow the scope of displayed metrics and charts.

Clicking a section of any chart will display an All Activity report with filters applied based on the selected chart section.

Audit Profiles

When you register a target database, Oracle Data Safe automatically creates an audit profile resource for your target database.

About Oracle Data Safe Audit Profiles

An audit profile defines the online retention period, offline retention period, and the paid usage settings for a target database. It can show you audit data volume to help you configure audit data collection in Oracle Data Safe. It's also responsible for automatically discovering audit trails in the target database during target registration. A target database has exactly one audit profile.

Audit Data Retention

Activity auditing collects audit records from audit trails for select target databases and copies the data into the Oracle Data Safe audit repository. The repository consists of online storage (available for immediate reporting and analysis) and offline storage (archive). The audit data retention feature helps you to manage the volume of audit data in the Oracle Data Safe database and in the archive.

There are two audit data retention settings that you need to configure for each target database: **online retention period** and **offline retention period**.

- The online retention period specifies the number of months to store audit data in online storage. The minimum online retention period is one month and the maximum is twelve months.
- The offline retention period specifies the number of months to store audit data in offline storage. The minimum offline retention period you can set is zero months and the maximum is 72 months (six years). Thus, you can archive audit data for a maximum of seven years in Oracle Data Safe from the time the audit record was generated on the target database (one year online and six years in the archive). If you have a requirement to store the audit data even longer in archive, please contact the Oracle Support.

Audit records are continuously collected from the target database and stored in Oracle Data Safe based on the total audit data retention period (in months), which is equal to the online retention period plus the offline retention period. For example, if you configure the online period to be three months and the archive period to be twelve months, the total audit data retention period is fifteen months. Audit records generated from the present date to three months ago are stored online. Audit records generated on the target database from four to fifteen months ago are archived.

> **Caution:**
>
> All other audit records are purged.

Audit Data Retrieval

Retrieval of audit data returns the audit data from offline archive storage to online Data Safe repository in order to make it available for online reports.

At any time, you can retrieve up to twelve months of archived audit data for each of your target databases. There is no requirement for the twelve month period to be consecutive. Retrieving audit data from the archive usually takes at least one hour.

Suppose you retrieve four months of archived data for a target database. You can do a second retrieval of up to eight months of archived data. If you drop the four months of retrieved data prior to doing the second retrieval, then you can retrieve twelve months of archived data. If you need to retrieve more than twelve months of archived data for any target database, you can file a service request with Oracle Support. In the service request, specify the increase in months needed and how long (in months) you need the increase to be in effect. The increased limit applies to all target databases in your tenancy.

You can retrieve audit data from the archive up to six times per month per target database. If needed, you can request an increase by filing a service request with Oracle Support. In the service request, specify how many more retrievals per month you require. The increased limit applies to all target databases in your tenancy.

Global Settings

Each regional Oracle Data Safe service has global settings for online retention period, archive retention period, and paid usage. Global settings are applied to all target databases unless their audit profiles override them.

If you want to modify the preferences for all targets, use Global Settings. If you want to modify preferences for a specific target database, use the audit profile settings for the target.

Paid Usage

Oracle Data Safe can collect an unlimited number of audit records per month per target database. The first one million audit records it collects per month per target database are free. Beyond that, you may incur charges. Please consult the Oracle Cloud price list.

You can enable or disable *paid usage* at a global or target database level. By default, paid usage is enabled at the global settings and all target databases inherit this global setting. This default setting allows Oracle Data Safe to continue collection beyond a million audit records per month per target database. You can override the global setting for a target database in its audit profile to disable paid usage.

If you want Oracle Data Safe to continue collecting audit data beyond the free monthly limit, you need to enable paid usage for the applicable target databases.

If you don't want Oracle Data Safe to continue collecting audit data beyond the free monthly limit, you need to disable paid usage for the applicable target databases. When the limit is reached, Oracle Data Safe stops collecting audit data from the target databases (by stopping the audit trails), and then resumes collection the following month.

Audit Data Volume

On an Audit Profile Details page, you can view monthly audit data volume, including the number of available audit records on your target database, the number of collected audit records in Oracle Data Safe that are available for online reporting, and the number of archived audit records in Oracle Data Safe. These numbers are intended to provide the information you need to configure audit data collection in Oracle Data Safe. Oracle Data Safe also uses them to calculate your monthly billing cycle. Audit records for actions performed by the Oracle Data Safe service account on a target database are excluded from the calculations.

The **Audit Records (current calendar month)** field on the Audit Profile Details tab shows number of audit records collected by Data Safe in the current calendar month. Audit records for the Data Safe service account on the target database are excluded and are not counted towards your monthly free limit. Monthly values are updated every 24 hours.

Under **Compute Audit Volume** on this page, you can compute available audit records on your target database for each audit trail that has not yet been collected by Oracle Data Safe. Here you can also compute the number of collected audit records in Oracle Data Safe that are available for online reporting, and the number of archived audit records in Oracle Data Safe. This helps provide the information you need to configure audit data collection in Oracle Data Safe.

Deregistered Target Databases

If you deregister a target database, the audit data collected for it in the Oracle Data Safe repository is retained according to how you set the online and offline retention periods before you deregistered the target database. Metadata for the deregistered target database is kept indefinitely.

Related Topics

- View and Manage Audit Profiles
  You can view audit profiles for target databases, update them, compute audit volume with them, move them to different compartments, and add tags to them.

Audit Policies

An audit policy represents all available audit policies relevant to a target database, along with their corresponding audit conditions and their provisioning status on the target database.

About Oracle Data Safe Audit Policies

When you register a target database, Oracle Data Safe automatically creates one audit policy resource for your target database. It does this after it retrieves the audit policies from the target database. The audit policy resource lets you provision unified audit policies within your target database, with conditional enablement of users and/or roles. It also enables you to retrieve the latest audit configurations from the target database in case these audit policies are modified within target database. The audit policies are also retrieved automatically by Oracle Data Safe once per day. Different categories of audit policies available for provisioning include:

- Basic auditing policies
- Administrator activity auditing policy
- User activity auditing policy
- Audit compliance standards policies
- Custom predefined audit policies
- Oracle predefined audit policies

Once the audit policy is provisioned to the target database, audit records are generated for activities within target database that match the audit policies. You can manage audit data volume in the target database by using the auto purge feature (which is disabled by default). You can also manage the audit data volume collected by Oracle Data Safe using audit data retention setting.

Notes:

- You have the flexibility to exclude activities performed by the Oracle Data Safe service account in the target database from auditing.
- Provisioning and retrieval of audit policies is not supported in Oracle Database 12.1 and below.

Basic Auditing Policies

Basic audit policies represent a set of recommended audit configurations for Oracle Database. You can enable the following basic auditing policies:

- Critical Database Activity
- Login Events
- Database Schema Changes

The **Critical Database Activity** policy allows you to audit critical database activity, for example, when a user, role, or profile is created, modified, or dropped.

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_ADS$_CRITICAL_DB_ACTIVITY
PRIVILEGES EXEMPT ACCESS POLICY,EXEMPT REDACTION POLICY,
        ADMINISTER KEY MANAGEMENT,EXPORT FULL DATABASE,IMPORT FULL DATABASE,
        CREATE PUBLIC DATABASE LINK, ALTER PUBLIC DATABASE LINK, DROP PUBLIC
DATABASE LINK,
        CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
        SELECT ANY DICTIONARY, ADMINISTER DATABASE TRIGGER,
        PURGE DBA_RECYCLEBIN, LOGMINING
ACTIONS CREATE USER, ALTER USER, DROP USER,
        CREATE ROLE, DROP ROLE, ALTER ROLE, SET ROLE, GRANT, REVOKE,
        CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
        CREATE PLUGGABLE DATABASE, DROP PLUGGABLE DATABASE, ALTER PLUGGABLE
DATABASE,
        CREATE LOCKDOWN PROFILE, ALTER LOCKDOWN PROFILE, DROP LOCKDOWN
PROFILE,
        ALTER DATABASE, ALTER SYSTEM,
        CREATE TABLESPACE, ALTER TABLESPACE, DROP TABLESPACE,
        CREATE ROLLBACK SEGMENT, ALTER ROLLBACK SEGMENT, DROP ROLLBACK
SEGMENT,
        CREATE DIRECTORY, DROP DIRECTORY,
         CREATE DISK GROUP,ALTER DISK GROUP,DROP DISK GROUP,
        CREATE PFILE,CREATE SPFILE
ACTIONS COMPONENT = datapump EXPORT,IMPORT
ACTIONS COMPONENT = DIRECT_LOAD LOAD;

AUDIT POLICY ORA_ADS$_CRITICAL_DB_ACTIVITY;
-- enabled for all users
```

The **Login Events** policy tracks all login and logoff activities by users. For more granularity, specify the trusted users to be excluded, irrespective of whether they are Oracle-maintained users or non-Oracle-maintained users.

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_ADS$_LOGON_EVENTS ACTIONS LOGON,LOGOFF;
CREATE AUDIT POLICY ORA_ADS$_LOGON_FAILURES ACTIONS LOGON;
AUDIT POLICY ORA_ADS$_LOGON_EVENTS EXCEPT <comma separated user list>;
AUDIT POLICY ORA_ADS$_LOGON_FAILURES whenever not successful;
```

The **Database Schema Changes** policy tracks all Data Definition Language (DDL) commands issued by any database user, for example, when a table, database link, function, or trigger is created, modified, or dropped.

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_ADS$_DB_SCHEMA_CHANGES
PRIVILEGES
         CREATE EXTERNAL JOB, CREATE JOB, CREATE ANY JOB
ACTIONS CREATE PROCEDURE, DROP PROCEDURE, ALTER PROCEDURE,
        CREATE PACKAGE, ALTER PACKAGE, DROP PACKAGE, CREATE PACKAGE BODY,
ALTER PACKAGE BODY, DROP PACKAGE BODY,
        CREATE FUNCTION, DROP FUNCTION, ALTER FUNCTION,
        CREATE TRIGGER, ALTER TRIGGER, DROP TRIGGER,
        CREATE LIBRARY, ALTER LIBRARY, DROP LIBRARY,
        CREATE SYNONYM, DROP SYNONYM,
        CREATE TABLE, ALTER TABLE, DROP TABLE, TRUNCATE TABLE,
         CREATE DATABASE LINK, ALTER DATABASE LINK, DROP DATABASE LINK,
        CREATE INDEX, ALTER INDEX, DROP INDEX,
        CREATE OUTLINE, ALTER OUTLINE,DROP OUTLINE,
        CREATE CONTEXT, DROP CONTEXT,
        CREATE ATTRIBUTE DIMENSION,ALTER ATTRIBUTE DIMENSION,DROP ATTRIBUTE
DIMENSION,
        CREATE DIMENSION,ALTER DIMENSION,DROP DIMENSION,
        CREATE INDEXTYPE,ALTER INDEXTYPE,DROP INDEXTYPE,
        CREATE OPERATOR,ALTER OPERATOR,DROP OPERATOR,
        CREATE JAVA,ALTER JAVA,DROP JAVA,
        CREATE MINING MODEL,ALTER MINING MODEL,DROP MINING MODEL,
        CREATE TYPE BODY,ALTER TYPE BODY,DROP TYPE BODY,
        CREATE TYPE,ALTER TYPE,DROP TYPE,
        CREATE MATERIALIZED VIEW,ALTER MATERIALIZED VIEW,DROP MATERIALIZED
VIEW,
        CREATE MATERIALIZED VIEW LOG, ALTER MATERIALIZED VIEW LOG,DROP
MATERIALIZED VIEW LOG,
        CREATE MATERIALIZED ZONEMAP, ALTER MATERIALIZED ZONEMAP,DROP
MATERIALIZED ZONEMAP,
        CREATE VIEW, ALTER VIEW, DROP VIEW,CREATE ANALYTIC VIEW, ALTER
ANALYTIC VIEW, DROP ANALYTIC VIEW,
        CREATE SEQUENCE, ALTER SEQUENCE, DROP SEQUENCE,
        CREATE CLUSTER, ALTER CLUSTER, DROP CLUSTER,TRUNCATE CLUSTER;

AUDIT POLICY ORA_ADS$_DB_SCHEMA_CHANGES;
-- enabled for all users
```

Admin Activity Auditing Policy

The Admin Activity Auditing policy lets you audit all activities by privileged administrators. These administrators can make significant changes to the wider system. A database administrator (DBA) can have access to sensitive data that is not protected by realms, and can exfiltrate. The Admin Activity auditing policy audits all activities for any user who has one of the following privileges or roles:

- **Admin privileges:**

  `SYSOPER`, `SYSDG`, `SYSKM`, `SYSRAC`, and `SYSBACKUP`

- **Roles:**

  `DBA`, `DATAPUMP_EXP_FULL_DATABASE`, `DATAPUMP_IMP_FULL_DATABASE`, `EXP_FULL_DATABASE`, `IMP_FULL_DATABASE`

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY "ORA_ADS$_ADMIN_USER_ACTIVITY" ACTIONS ALL WHEN
'SYS_CONTEXT(''USERENV'', ''CURRENT_USER'') NOT IN
(''CTXSYS'',''ORDSYS'',''OJVMSYS'',''DVSYS'',''SI_INFORMTN_SCHEMA'',''AUDSYS''
,''GSMADMIN_INTERNAL'',''ORDPLUGINS'',''DIP'',''MDSYS'',
''OLAPSYS'',''ORDDATA'',''LBACSYS'',''SYSKM'',''OUTLN'',''ORACLE_OCM'',''SYS$U
MP'',''SYSRAC'',''ANONYMOUS'',''GGSYS'',''REMOTE_SCHEDULER_AGENT'',
''SYSBACKUP'',''DBSFWUSER'',''MDDATA'',''APPQOSSYS'',''DBSNMP'',''GSMUSER'',''
GSMCATUSER'',''XS$NULL'',''SYSTEM'',''SYS'',''SYSDG'',
''WMSYS'',''XDB'',''DVF'')' EVALUATE PER STATEMENT ONLY TOPLEVEL

AUDIT POLICY ORA_ADS$_ADMIN_USER_ACTIVITY BY USERS WITH GRANTED ROLES DBA,
DATAPUMP_EXP_FULL_DATABASE, DATAPUMP_IMP_FULL_DATABASE, EXP_FULL_DATABASE,
IMP_FULL_DATABASE;

AUDIT POLICY ORA_ADS$_ADMIN_USER_ACTIVITY BY PUBLIC, SYSDG, SYSKM, SYSRAC,
SYSBACKUP;
```

> **Note:**
>
> The `ORA_ADS$_ADMIN_USER_ACTIVITY` policy requires support for `TOPLEVEL`, which is included starting in Oracle Database 19c. For databases older than Oracle Database 19c, ensure the required patch from My Oracle Support is applied as a prerequisite to provisioning this policy to the target database.
>
> 1. Login to My Oracle Support.
> 2. Click the **Patches & Updates** tab.
> 3. Search for patch number 21493004 and platform Linux x86-64.
> 4. Select and download the patch that corresponds to the Oracle Database release of the target database.

For Oracle Database 19c, the following audit policy also gets provisioned:

```
CREATE AUDIT POLICY ORA_ADS$_SYS_TOP_ACTIVITY ACTIONS ALL ONLY TOPLEVEL;
AUDIT POLICY ORA_ADS$_SYS_TOP_ACTIVITY by SYS;
```

User Activity Auditing Policy

The User Activity Auditing policy tracks all user-initiated activities by users who may have access to sensitive data or broader access to the database. Be sure that you specify which users to audit. These users could be “non-admin but privileged” users. When enabling this policy in the interface, you must specify non-Oracle maintained users to audit.

The following audit policy gets provisioned on the target database:

```
CREATE AUDIT POLICY ORA_ADS$_USER_ACTIVITY ACTIONS ALL
WHEN 'SYS_CONTEXT(''USERENV'', ''CURRENT_USER'') NOT IN
(''DIP'',''WMSYS'',''XDB'',''ORDDATA'',''OLAPSYS'',''MDSYS'',''ORDPLUGINS'',''
GSMADMIN_INTERNAL'',''SI_INFORMTN_SCHEMA'',''ANONYMOUS'',''GGSYS'',''DBSFWUSER
'',''APPQOSSYS'',''DBSNMP'',''GSMUSER'',''SYSDG'',''SYS$UMF'',''ORACLE_OCM'','
'OUTLN'',''SYSKM'',''SYS'',''SYSTEM'',''XS$NULL'',''GSMCATUSER'',''MDDATA'',''
SYSBACKUP'',''REMOTE_SCHEDULER_AGENT'',''SYSRAC'',''CTXSYS'',''DVF'',''OJVMSYS
'',''DVSYS'',''AUDSYS'',''ORDSYS'',''LBACSYS'')' EVALUATE PER STATEMENT ONLY
TOPLEVEL;

AUDIT POLICY ORA_ADS$_USER_ACTIVITY BY <comma-separated non-Oracle maintained
user list>
```

This audit policy is intended for non-Oracle users whose activity needs to be monitored. The policy excludes the following Oracle users:

ANONYMOUS	DVF	MDDATA	ORDSYS	SYSDG
APPQOSSYS	DVSYS	MDSYS	OUTLN	SYSKM
AUDSYS	GGSYS	OJVMSYS	REMOTE_SCHEDULER_AGENT	SYSRAC
CTXSYS	GSMADMIN_INTERNAL	OLAPSYS	SI_INFORMTN_SCHEMA	SYSTEM
DBSFWUSER	GSMCATUSER	ORACLE_OCM	SYS	WMSYS
DBSNMP	GSMUSER	ORDDATA	SYS$UMP	XDB
DIP	LBACSYS	ORDPLUGINS	SYSBACKUP	XS$NULL

> **Note:**
>
> The `ORA_ADS$_USER_ACTIVITY` policy requires support for `TOPLEVEL`, which is included starting in Oracle Database 19c. For databases older than Oracle Database 19c, ensure the required patch from My Oracle Support is applied as a prerequisite to provisioning this policy to the target database.
>
> 1. Login to My Oracle Support.
> 2. Click the **Patches & Updates** tab.
> 3. Search for patch number 21493004 and platform Linux x86-64.
> 4. Select and download the patch that corresponds to the Oracle Database release of the target database.

Custom Policies

Custom policies represent set of custom audit policies that defines audit configurations unique to your scenario, for example tracking sensitive data access. You can create custom audit policies in the target database and Oracle Data Safe retrieves them. You can then enable or disable them.

Oracle Predefined Policies

Oracle predefined policies represent a set of pre-designed best practice audit policies provided by Oracle Database. They cover audit settings that are commonly relevant to security.

> **See Also:**
>
> Because predefined unified audit policies vary in Oracle Database releases, check the list of these policies in the version of the *Oracle Database Security Guide* that is appropriate to your target database. For example, if your target is an Oracle Database 19c database, see Auditing Activities with the Predefined Unified Audit Policies.

Oracle predefined policies are retrieved from the target database by Oracle Data Safe. The following are examples. Depending on your target database, such as Autonomous Transaction Processing (serverless) and Autonomous Data Warehouse, you may have more predefined policies in addition to those listed below.

- `ORA_ACCOUNT_MGMT`
- `ORA_DATABASE_PARAMETER`
- `ORA_SECURECONFIG`
- `ORA_DV_AUDPOL`
- `ORA_DV_AUDPOL2`
- `ORA_RAS_POLICY_MGMT`
- `ORA_RAS_SESSION_MGMT`

- ORA_LOGON_FAILURES
- COMMON_USER
- ADB_ADMIN_AUDIT
- ADB_MANDATORY_AUDIT

Audit Compliance Standards

Audit compliance standards represent a set of audit policies that helps accelerate compliance to regulatory standards. They also help you evaluate whether you are adhering to database compliance requirements.

During Activity Auditing, you can enable or disable two audit compliance standards policies:

- Center for Internet Security (CIS) Configuration - available for Oracle Database 12.2 and later
- Security Technical Implementation Guidelines (STIG) - available for Oracle Database 21c and later

These policies track many activities and can help you evaluate whether you are adhering to database compliance requirements. For example, you can track when a user, database link, profile, or procedure is created, altered, or dropped.

The Center for Internet Security (CIS) Recommendations policy (ORA_CIS_RECOMMENDATIONS) is a predefined unified audit policy in Oracle Database designed to perform audits that the CIS recommends. CIS is a world-recognized organization that provides consensus-based best practices for helping organizations assess and improve their cyber security posture. They provide resources, such as configuration assessment tools, secure configuration benchmarks, security metrics, and certifications. One of the main objectives of the organization is to help businesses prioritize what they need to do for security, and they strive to provide recommendations in simple, non-technical terms.

STIG is a set of rules, checklists, and other best practices created by the Defense Information Systems Agency (DISA) to ensure compliance with Department of Defense (DOD)-mandated security requirements.

Related Topics

- View and Manage Audit Policies
  You can view and provision audit policies, update the list of available audit policies, update users and roles for audit policies, move audit policies to different compartments, and add tags to audit policies.

Audit Trails

An audit trail represents the collection of audit records from the target database trail such as UNIFIED_AUDIT_TRAIL, which provides documentary evidence of the sequence of activities that happen.

A database audit trail is the source of audit records showing what has happened in the target database. When audit data collection is enabled for the specified database audit trail in an audit trail resource, the audit records are copied from the database's audit trail into Oracle Data Safe in near-real time. You can manage the audit records volume in the target database using the auto purge feature.

About Oracle Data Safe Audit Trails

An audit trail is an audit table in a target database that stores audit data. The most common audit trail is the UNIFIED_AUDIT_TRAIL data dictionary view, which consolidates all Oracle Database audit trails into one location and in a unified format.

During target database registration, Oracle Data Safe automatically discovers the audit trails on a target database and creates one audit trail resource per target database audit trail. These audit trail resources are listed on the Audit Trails page in Security Center. You can discover new audit trails for a target database at any time and remove audit trail resources in Oracle Data Safe as needed.

When you start an Oracle Data Safe audit trail, Oracle Data Safe begins copying audit records from the target database audit trail into the Oracle Data Safe repository. You can start and stop audit data collection as needed. In most cases, you configure Oracle Data Safe to collect audit data from only one audit trail in your target database, although it is possible to collect from more than one.

Supported Target Database Audit Trails

The following table lists the target database audit trails that Oracle Data Safe can discover. The SQL_TEXT, SQL_BINDS, and RLS_INFO columns in UNIFIED_AUDIT_TRAIL and SYS.AUD$ are truncated to 32KB before being stored in Oracle Data Safe. So are LSQLTEXT, LSQLBIND, and RLS$INFO in SYS.FGA_LOG$.

Unified audit policy retrieval and provisioning in Oracle Data Safe is supported only on Oracle Database versions 12.2 and above. Traditional audit settings cannot be retrieved and provisioned from Oracle Data Safe,although you can choose to do so within the target database and configure traditional audit trails for collection.

Database Version	Standard Edition	Enterprise Edition
Non-Autonomous Databases, versions 11.2.0.4, 12.1.0.1, 12.1.0.2	SYS.AUD$	SYS.AUD$ SYS.FGA_LOG$* DVSYS.AUDIT_TRAIL$ (when Database Vault is enabled)

Database Version	Standard Edition	Enterprise Edition
Non-Autonomous Databases, versions 12.2 and above	UNIFIED_AUDIT_TRAIL SYS.AUD$	UNIFIED_AUDIT_TRAIL** SYS.AUD$ SYS.FGA_LOG$* DVSYS.AUDIT_TRAIL$ (when Database Vault is enabled)
Autonomous Databases (latest version)	(not applicable)	UNIFIED_AUDIT_TRAIL**

Note:

SYS.AUD$, SYS.FGA_LOG$*, and DVSYS.AUDIT_TRAIL$ are available in mixed mode only.

*When you enable auto-purge for an FGA_LOG$ audit trail, you may encounter an error and the audit trail is in a stopped state. To enable auto purge, re-run the datasafe_privileges.sql on the target database and restart the audit trail.

For Active Data Guard associated target databases, you will see:

- A UNIFIED_AUDIT_TRAIL collecting records from the AUDSYS.AUD$UNIFIED table of the primary database. For example, TABLE:PRIMARY.
- A UNIFIED_AUDIT_TRAIL collecting audit records from the operating system spillover files of the primary database. For example, FILE:database_unique_name1.
- A UNIFIED_AUDIT_TRAIL collecting audit records from the operating system spillover files of each peer database that is registered. For example, FILE:database_unique_name2.

You can distinguish the UNIFIED_AUDIT_TRAIL that point to the operating system spillover files by the associated database unique name.

Auto Purge

It is important to properly manage audit data volume on your databases to ensure efficient performance and optimum use of the disk space. As audit trails on your databases grow in volume, querying the audit trail with large volume of audit data may impact performance and lead to space scalability issues. It is best to purge old audit records from the database audit trail periodically after they are collected by Oracle Data Safe. This is why you may want to consider using the auto purge feature.

The Oracle Data Safe auto purge feature in Activity Auditing lets you purge audit records from your target databases on a regularly scheduled basis. The auto purge feature is an operation on a target database. When auto purge is enabled for a target database, a daily job runs that looks at the last archive timestamp and deletes all the audit records that are seven days older

than the timestamp value. Data Safe manages the audit data retention in the target database, including updating the last archive timestamp after each collection.

> **Caution:**
>
> Enabling auto purge deletes all audit records in the target database audit trail every seven days, including those older than the initial start date of the audit collection. Records might be deleted even if they are not collected in Oracle Data Safe. After considering this impact, you should enable this feature carefully.
>
> Additionally, the purging of audit records in a database target should only be managed through Data Safe. Although Data Safe collects audit records frequently, purging audit data from outside the Data Safe framework (for example, manually running `DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL`) has the potential to delete audit records that Data Safe has not yet collected. If you have created a custom job to periodically purge audit data, you should consider deleting or disabling that job to avoid conflicts in purge activity.

If you enable auto purge and want to see additional details like `purgeJobTime`, `purgeJobStatus`, and `purgeJobDetails`, re-run the `datasafe_privileges.sql` script for `AUDIT_COLLECTION` on the target database. See Grant Roles to the Oracle Data Safe Service Account on Your Target Database for more information.

Auto purge is disabled by default. Even if you disable auto purge in Oracle Data Safe, be aware that your target database may still be purging audit data based on the target database's audit data retention settings. Please refer to your database's documentation for details.

Related Topics

- View and Manage Audit Trails
  You can view details for an audit trail in Oracle Data Safe, start an audit trail to begin collecting audit data, start and stop an audit trail as needed, enable or disable the auto purge feature for an audit trail, and delete an audit trail.

Configure Auditing and Alerts

You can configure auditing and alerts or start audit trails by using the wizard in Activity Auditing.

Start Audit Trails Through Activity Auditing

1. Under **Security center**, click **Activity auditing**.
2. Click **Start audit trails**.
3. Select a target database. If the database is not in the displayed compartment, click **Change compartment**, select the correct compartment, and then choose the target database from that compartment.
4. If you wish to start collecting all the existing audit data in a particular audit trail, select the audit trail check box. Note: only trails that are in a `NOT_STARTED` or `STOPPED` state will be displayed as options.
5. Select a start date. This date will be applied to all trails selected. Note: if a trail is in a `STOPPED` state, it will resume from when it was stopped, not the new start date.

6. To review audit volume before starting the audit trail, click **Configure auditing and alerts**.
7. Click **Start trail(s)**. The **Collection state** field shows as **COLLECTING** when the audit trail is in IDLE, COLLECTING or RECOVERING state. You can view the actual state (sub-state) in the work request details section.

Run the Configure Auditing and Alerts Wizard

From the **Activity Auditing** dashboard, you can configure auditing and alerts. This is the workflow:

1. Under **Security center**, click **Activity auditing**.
2. Click **Configure auditing and alerts**.

Step 1: Alert Policy

1. Under **Security center**, click **Activity auditing**.
2. Click **Configure auditing and alerts** to begin the wizard.

   The wizard displays the **Configure auditing and alerts for the target database** page.
3. Select a target database. If the database is not in the displayed compartment, click **Change compartment**, select the correct compartment, and then choose the target database from that compartment.
4. Select one or more alert policies for the target database. Any currently applied alert policies will already be selected, if applicable.
5. Click **Next**.

Step 2: Audit Policy

1. Review the current audit policies and make any necessary changes for the target database. Note: policies that are pre-selected and grayed out are required.
2. If you wish to edit user activity, click the corresponding **Enabled for all users** or **Enabled for specific users and/or roles** link.
   a. The Configure policy window will appear. Choose which users to enable the policy for: **All users**, **Only a specific set of users and/or roles**, or **All users except a specific set of users**.
   b. If you wish to add a specific set of users, click **Add users/roles**.
   c. Select either **Users** or **Roles**.
   d. If you selected **Users**, select the list of users.
   e. For **Operational status**, select either **Success**, **Failure**, or **Success or failure**.
   f. Click **Save**.
3. Click **Next**.

Step 3: Audit Trails

1. Select the audit trail(s) you want to start for the target database.
2. (Optional) Click **Calculate audit records for additional months**.

3. The **Show number of available audit records** window will appear. Select a start date, which will only apply to audit trails that have not been previously started.
4. Click **Show**.
5. Click **Next**.

Step 4: Audit Profile

1. Specify the number of months the audit records will be stored online in the Data Safe audit repository for immediate reporting and analysis. The minimum is 1 month, and the maximum is 12 months.
2. Specify the number of months the audit records will be stored offline in the Data Safe audit archive. The minimum is 0 months, and the maximum is 72 months. If you have a requirement to store the audit data even longer in the archive, contact Oracle Support.
3. If applicable, confirm whether you want to override the global retention settings. Note: Selecting **No** will reset the retention values to the global settings.
4. Select **Paid usage (Audit records > million/month)** if you want to continue collecting audit records beyond the free limit of one million audit records per month per target database.
5. If applicable, confirm whether you want to override the global paid usage settings. Note: Selecting **No** will reset the paid usage values to the global settings.
6. Click **Next**.

Step 5: Review and Submit

1. Review and confirm the changes for the target database.
2. To modify a specific change, click **Edit** to return to any previous step.
3. Click **Next**.

Step 6: Audit Configuration Progress

1. The audit configuration will begin. Stay on the page to see the progress.
2. Click **Close**.

View and Manage Global Settings for Oracle Data Safe

There are several global Oracle Data Safe settings that you can control.

View Global Settings

1. Access the **Overview** page for Oracle Data Safe.
2. Under **Data Safe** on the left, click **Settings**. The **Default Settings** page for the region is displayed.
3. View the default settings for global paid usage and the global retention policy.

Enable or Disable Global Paid Usage

> **Note:**
>
> By default, Oracle Data Safe allows audit collection to continue after the free one million audit records limit is reached within a month.

You can disable or enable Global Paid Usage. When paid usage is disabled for a target, Oracle Data Safe automatically stops collecting audit records on a target database after the free limit is reached for a month. It resumes collection the next month, and resets the audit record count back to zero. If you want to change whether or not Oracle Data Safe continues to collect audit data on all of your target databases beyond the free limit, you can do so on the **Settings** page.

1. Access the Oracle Data Safe home page.
2. On the left under **Data Safe**, click **Settings**. The **Default Settings** page is displayed.
3. In the **Global Paid Usage Settings** section, select or deselect **Continue audit data collection for target databases beyond the monthly free limit**. If you want to continue collection beyond the free limit and are willing to accept the additional cost, ensure that this option is selected. By default, it is selected.
4. Click **Save**.

Set Global Retention Periods

You can set the global online and archive retention periods on the **Settings** page in Oracle Data Safe.

1. Access the Oracle Data Safe home page.
2. On the left under **Data Safe**, click **Settings**. The **Default Settings** page is displayed.
3. In the **Global Retention Policy** section, enter the online retention period and archive retention periods in months.
   - Records stored online are available in the audit reports for a minimum of 1 month and a maximum of 12 months.
   - Archived records are not immediately available in the audit reports. However, if you need them to be, you can retrieve them back online. They are retained in archive for a minimum of 0 months and a maximum of 72 months. If you have a requirement to store the audit data even longer in archive, please contact Oracle Support.
4. Click **Save**.

View and Manage Audit Profiles

You can view audit profiles for target databases, update them, compute audit volume with them, move them to different compartments, and add tags to them.

Audit Profile Details

You can view the following information in an audit profile:

- Profile name (editable)
- Target database to which the audit profile belongs
- Profile description (editable)
- Profile Oracle Cloud Identifier (OCID)
- When the audit profile was created and last updated
- Compartment in which the audit profile resides. This is always the same compartment to which the target database was registered.
- Whether the option to override the global paid usage setting is selected
- Whether paid usage is selected for the target database
- Whether the option to override the global retention period is selected
- Online and offline retention periods
- Audit volume (number of audit records collected by Oracle Data Safe from the target database that are applied to the current month's billing cycle)
- Available audit trail locations

> **Note:**
>
> For Active Data Guard associated target databases, you will see:
>
> – A `UNIFIED_AUDIT_TRAIL` collecting records from the `AUDSYS.AUD$UNIFIED` table of the primary database. For example, `TABLE:PRIMARY`.
>
> – A `UNIFIED_AUDIT_TRAIL` collecting audit records from the operating system spillover files of the primary database. For example, `FILE:database_unique_name1`.
>
> – A `UNIFIED_AUDIT_TRAIL` collecting audit records from the operating system spillover files of each peer database that is registered. For example, `FILE:database_unique_name2`.
>
> You can distinguish the `UNIFIED_AUDIT_TRAIL` that point to the operating system spillover files by the associated database unique name.

- Tags
- Monthly available data in the target database
- Monthly collected online audit data in Oracle Data Safe
- Monthly collected offline audit data in Oracle Data Safe

View an Audit Profile for a Target Database

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.

4. On the right, click the name of the target database for which you want to view audit profile details. The **Audit Profile Details** page for the selected target database is displayed.
5. On the **Audit Profile Details** tab, view information about the audit profile.
6. To view the monthly available audit data in the target database, collected online audit data in Oracle Data Safe, and collected offline data in Oracle Data Safe, scroll down and view the table in the **Compute Audit Volume** section.

> **Note:**
>
> You can also discover new audit trails for a target database from the **Audit Profiles Details** page. See Discover Audit Trails for a Target Database

Update the Name and Description of an Audit Profile

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. (Optional) Under **Filters**, select a target database from the **Target databases** list to narrow the scope of displayed metrics.
4. On the right, click the name of the target database.
5. To change the name of the audit profile, click the pencil icon next to the profile name and then enter the new name.
6. To change the description of the audit profile, click the pencil icon next to the profile description, edit the description and click the save icon.

Override Global Retention Period for a Target Database

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of the target database for which you want to update the retention period. The audit profile for the selected target database is displayed.
4. Click **Update Retention**. The **Update Retention** dialog box is displayed.
5. Select **Yes** at **Do you want to override the global retention settings?**.

   Your configuration will override the global retention policy settings for your target database.
6. For **Online Retention**, enter the number of months you want to store audit data online for immediate analysis.
7. For **Offline Retention**, enter the number of months that you want to store audit data offline.
8. (Optional) Depending on how much audit data you have, there may be additional costs. Click the **Pricing Details** link to learn more.
9. Click **Update Retention**.

Compute Available Audit Volume on a Target Database

You can query and view the monthly number of audit records collected on your target database from a particular date and time. It is possible to show audit records available in the target database. but not collected yet in Oracle Data Safe. Knowing how many audit records exist on your target database and when the records were generated can help you to determine when to start collecting audit records in Oracle Data Safe and manage the billing.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of your target database. The audit profile for the selected target database is displayed.
4. Scroll down to the **Compute Audit Volume** section.
5. Click **Available on Target Database**. The **Compute Available Volume** dialog box is displayed.
6. For **Select Start Date**, click the box and configure a start date and time from which you want to view the available volume. Oracle Data Safe will list the audit records collected on your target database for each month following the date that you set here.
7. Click **Compute**. The number of audit records collected on your target database is updated next to each audit trail. For example, you might see a value like `0.4M` next to `UNIFIED_AUDIT_TRAIL`, which means there are 0.4 million individual audit records collected in the `UNIFIED_AUDIT_TRAIL` on your target database.

   For Active Data Guard associated target databases, you will see:

   - A `UNIFIED_AUDIT_TRAIL` collecting records from the `AUDSYS.AUD$UNIFIED` table of the primary database. For example, `TABLE:PRIMARY`.
   - A `UNIFIED_AUDIT_TRAIL` collecting audit records from the operating system spillover files of the primary database. For example, `FILE:database_unique_name1`.
   - A `UNIFIED_AUDIT_TRAIL` collecting audit records from the operating system spillover files of each peer database that is registered. For example, `FILE:database_unique_name2`.

   You can distinguish the `UNIFIED_AUDIT_TRAIL` that point to the operating system spillover files by the associated database unique name.

Compute Collected Audit Volume for a Target Database

You can query and view the monthly number of audit records collected by Oracle Data Safe for your target database for a specific time period.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of your target database. The audit profile for the selected target database is displayed.
4. Scroll down to the **Compute Audit Volume** section.
5. Click **Compute Collected Volume**. The **Compute Collected Volume** dialog box is displayed.

6. For **Start Month**, configure a start month from which you want to view the number of audit records.
7. For **End Month**, configure an end month.
8. Click **Compute**. The number of audit records collected by Oracle Data Safe is updated in the Collected in **Data Safe (Online)** column in the table.

Override Global Paid Usage for a Target Database

You can choose to collect or not collect audit records beyond the free limit of one million audit records per month per target database. Additional charges may apply. By default, all target databases will inherit the global paid usage settings, but this can be overridden for each target database.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of your target database for which you want to opt in for paid usage. The audit profile for the selected target database is displayed.
4. Click **Update Paid Usage**. The **Update Paid Usage** dialog box is displayed.
5. Select **Yes** at **Do you want to override the global paid usage settings?**.
6. Select or deselect **Paid Usage**.
7. Click **Update Paid Usage**.

Move an Audit Profile

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit profiles**.
3. On the right, click the name of the target database that has the audit profile that you want to move. The audit profile for the selected target database is displayed.
4. Click **Move resource**. The **Move resource** dialog box is displayed.
5. From the drop-down list, select a destination compartment.
6. Click **Move resource**. The audit profile is moved immediately.

Add Tags to an Audit Profile

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of the target database that has the audit profile to which you want to add tags The audit profile for the selected target database is displayed.
4. Click **Add Tags**. The **Add Tags** dialog box is displayed.
5. Configure one or more tags, and then click **Add Tags**.

View and Manage Audit Trails

You can view details for an audit trail in Oracle Data Safe, start an audit trail to begin collecting audit data, start and stop an audit trail as needed, enable or disable the auto purge feature for an audit trail, and delete an audit trail.

Discover Audit Trails for a Target Database

You can discover new audit trails for a target database from the **Audit Profiles Details** page.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Profiles**.
3. On the right, click the name of the target database for which you want to discover audit trails. The audit profile for the selected target database is displayed.
4. Click **Discover Trails**. The **Discover Trails** dialog box is displayed.
5. Click **Confirm**. Any new audit trails for the target database that weren't discovered during target registration are discovered and listed on the **Audit Profiles Details** page under **Available Trail Locations**.
6. (Optional) To view details for an audit trail, click the name of an audit trail. The **Audit Trail Details** page is displayed, showing you the details for the audit trail.

Here are some situations where you might consider running the discover trails operation:

- If your target database has been upgraded from any version Oracle Database from 11g to 19c, then `UNIFIED_AUDIT_TRAIL` will be newly discovered by this operation.
- If the target database is Oracle Database 12c and above and is using traditional auditing (`SYS.AUD$`), and database administrator enables mixed mode auditing, then `UNIFIED_AUDIT_TRAIL` will be newly discovered by this operation.
- If the database administrator configures any additional audit trails are configured in the Oracle Database such as Database Vault audit trail or FGA audit trail, then these will be discovered in Oracle Data Safe if you run this operation.
- If you are running Amazon RDS for Oracle, audit trail is `None` by default. See Security auditing in Amazon RDS for Oracle and Working with DB parameter groups from Amazon to configure the parameter group for audit so that you can use the Audit Trail functionality of Oracle Data Safe.
- If you are adding a peer target database to a registered primary Active Data Guard target database after you've already discovered audit trails on the primary database, running the discovery trails operations will discover new trails associated with this newly added peer.

Audit Trail Details

Each audit trail in Oracle Data Safe has the following information:

- **Trail name** (editable)
- **Target database** - Target database to which the audit trail applies
- **Trail location** - Audit trail on the target database
- **Trail description** (editable)

- **Trail OCID** - Oracle Cloud Identifier for the audit trail object in Oracle Cloud Infrastructure
- **Compartment** - Compartment in Oracle Cloud Infrastructure in which the associated target database is stored
- **Profile name** - Audit profile name for the target database
- **Created time** - Date and time when the audit trail was created (UTC)
- **Updated time** - Date and time when the audit trail was last updated (UTC)
- **Collection state** - Values are blank if audit collection hasn't started yet
  - `COLLECTING` - trail is actively collecting audit records
  - `IDLE` - trail can't find any further records on the database to collect and is waiting for new audit records to be generated
  - `NOT_STARTED` - trail has been created when the target database has been registered
  - `RECOVERING` - trail has encountered an error and is trying to come back to `COLLECTING` state. The audit trail will have to re-process some of the audit records to avoid collecting them again.
  - `RESUMING` - trail is in the process of going to `COLLECTING` again after being stopped
  - `RETRYING` - trail is trying to enter `RESUMING` state
  - `STARTING` - trail is starting for the first time before moving to `COLLECTING`
  - `STOPPED` - trail has been manually stopped and not collecting audit records
  - `STOPPING` - trail has been manually stopped and is about to be `STOPPED`
  - `STOPPED_FAILED` - the target database for the audit trail has been deleted
  - `STOPPED_NEEDS_ATTN` - trail encountered a non-recoverable error on the target database and requires intervention to correct the error and resume

  .
- **Collection start time** - Data and time when audit collection started. This field is blank only when the audit trail has never been started.
- **Auto purge** - Whether the auto purge feature is enabled for the audit trail. Values are **Yes** or **No**.
- **Purge job status*** - Current status of the audit trail purge job. Values are **`SUCCEEDED`** or **`FAILED`**.
- **Purge job last execution time*** - Date and time of the last purge job (UTC). The purge job deletes audit data in the target database every seven days to prevent the database's audit trail from becoming too large.
- **Purge job details*** - Details of the audit trail purge job that ran at the time specificed in the **Purge job last execution time** column.
- **Trail Source** - For audit trails for Active Data Guard associated target databases, this states if the trail source is a `TABLE` or `FILE`.
- **Database unique name** - For audit trails for Active Data Guard associated target databases, this states the unique name of the primary database associated with the peer target database.
- **Profile name** - Name of the associated audit profile.
- **Policy name** - Name of the associated audit policy.

- **Work requests** - Operations running in Oracle Cloud Infrastructure that have to do with the audit trail

* To see this information you will need to re-run the `datasafe_privileges.sql` script for `AUDIT_COLLECTION` on the target database. See Grant Roles to the Oracle Data Safe Service Account on Your Target Database for more information.

View an Audit Trail

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   For each audit trail in Oracle Data Safe, you can view the target database name, the audit trail name, whether or not the audit trail needs attention, source audit trail location (for example, `SYS.AUD$` or `UNIFIED_AUDIT_TRAIL`), collection state, when the target database was registered, when audit data collection started, and whether auto purge is enabled.

   The **Audit Trails** page is displayed, tabling all of the audit trails to which you have access.
3. (Optional) Under **Filters** select a target database from the **Target Databases** list to narrow the scope of displayed audit trails.
4. (Optional) Under **Filters** select a collection state from the **Collection State** list to narrow the scope of displayed audit trails.
5. On the right, locate the audit trails for your target database. You can refer to the **Trail Location** column to distinguish between the different source audit trails.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.
6. To view more information about an audit trail, click the name of your target database on the audit trail's row.

   The **Audit Trail Details** page is displayed.
7. View the details for the audit trail.

Start an Audit Trail

Starting an audit trail for a target database is the same as starting audit collection. You can collect audit data that was created as far back as the data retention period.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   The **Audit Trails** page is displayed.
3. Click the name of your target database on the row for the audit trail that you want to start.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.
4. Click **Start**.

   The **Start Audit Trail** dialog box is displayed.
5. Click the **Select Start Date** box and select a date and time.
6. (Optional) To enable the auto purge feature, select **Auto Purge**.
7. Click **Start**.

The **Collection state** field shows as **COLLECTING** when the audit trail is in IDLE, COLLECTING or RECOVERING state. You can view the actual state (sub-state) in the work request details section.

For audit trials pointing to an operating system spillover file of an Active Data Guard associated database, it may take some time for the audit trail to start collecting.

Stop an Audit Trail

If an audit trail is reaching the monthly limit and exceeding that limit is a concern, you may want to stop the audit trail in order to avoid additional charges. You can override the default Paid Usage setting at the target level to stop collection of audit records for the current month once the limit is reached. Then the audit trail will resume collection at the start of the billing cycle in the next month.

If you use the Paid Usage option, there is no need to manually stop and start audit record collection for this purpose.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   The **Audit Trails** page is displayed.
3. Click the name of your target database on the row for the audit trail that you want to stop.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.
4. Click **Stop**. A dialog box is displayed, asking you to confirm.
5. Click **Yes**.

   Audit data collection into the audit trail is immediately stopped.

Resume Audit Data Collection

You can resume audit trails whose collection state is `STOPPED`.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   The **Audit Trails** page is displayed.
3. Click the name of your target database on the appropriate audit trail row.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.
4. Click **Resume**.

Update Auto Purge

You can enable or disable auto purge for a target database at any time.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   The **Audit Trails** page is displayed.

3. Click the name of your target database on the appropriate audit trail row.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.

4. Click **Update Auto Purge**.

   The **Update Auto Purge** dialog box is displayed.

5. Select **Auto Purge** to enable it for the target database or deselect it to disable it.

6. Click **Update Auto Purge**.

   The auto purge is immediately enabled or disabled in Oracle Data Safe. The auto purge job on the target database will be eventually created when audit trail is active.

> **Note:**
>
> The audit records collected for a deleted trail will be archived and purged according to retention policy. Creating the same trail again in Oracle Data Safe might result into duplicate collection of records.

Delete an Audit Trail

Oracle Data Safe automatically discovers all the audit trails on your target database during target database registration. In Oracle Data Safe, you can delete the audit trails that your target database is not using.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Trails**.

   The **Audit Trails** page is displayed.

3. Click the name of your target database on the appropriate audit trail row.

   For `UNIFIED_AUDIT_TRAIL`s pointing to the operating system spillover file of Active Data Guard associated target databases, you will see a database icon next to the trail location.

4. From the **More Actions** menu, select **Delete**.

   A **Delete Trail** dialog box is displayed.

5. Click **Delete Trail** to confirm.

   The audit trail is permanently deleted.

View and Manage Audit Policies

You can view and provision audit policies, update the list of available audit policies, update users and roles for audit policies, move audit policies to different compartments, and add tags to audit policies.

Audit Policy Details

Each Oracle Data Safe audit policy stores the following details:

- Policy name

- Target database to which the audit policy belongs
- Policy description
- Policy Oracle Cloud Identifier (OCID)
- Compartment in which the audit policy resides
- Details for basic, admin, user, custom, compliance, and predefined policies. A green circle means that the policy is enabled. A grey circle means that the policy is disabled. A statement indicates whether the policy is enabled for all users, specific users, and/or roles.

View an Audit Policy

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Policies**.
3. On the right, click the name of the target database for which you want to view the audit policy.

   The **Audit Policies Details** page is displayed.
4. On the **Audit Policy Details** tab, view policy details.
   - A green circle means that the policy is enabled.
   - A grey circle means that the policy is disabled.
   - A statement indicates whether the policy is enabled for all users, specific users, and/or roles.

Provision or Disable Audit Policies on a Target Database

For database version-related limitations, please see Supported Target Databases.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Policies**.
3. On the right, click the name of your target database on which you want to provision an audit policy.

   The **Audit Policies Details** page is displayed.
4. Click **Provision**.

   The **Provision Audit Policies** panel is displayed.
5. Note the **Data Safe User Activity Excluded** option on this page. If selected, then Oracle Data Safe user activity is not audited in this policy.

> **Note:**
>
> Exclusion will fail for the following instances:
>
> - RDBMS mandatory auditing
> - Compliance policies, such as STIG and CIS
> - Any custom audit policies that are provisioned exclusively on the Data Safe user
> - Any audit policies that audit a role that is already assigned to the Data Safe user
> - Audit records generated by a traditional audit trail

6. Select the audit policies that you want to provision on the target database. Deselect audit policies that you want to disable.
7. (Optional) Configure the audit policy for specific users or roles:
   a. Manually **Refresh database users** if there have been changes to the users of the target databases since the listed time.
   b. Click the **Enabled for all users** or **Enabled for specific users and/or roles** link.

      The **Configure Policy** window is displayed.
   c. Select one of the following options. The options in the dialog box change according to your selection.
      - **All users**
      - **Only a specific set of users and/or roles**
      - **All users except a specific set of users**
   d. If you selected **All users**, then for **Audit when operations**, select **Success**, **Failure**, or **Success or Failure**.
   e. If you selected **Only a specific set of users and/or roles**, click **Add Users/Roles**.

      If you add the Data Safe service account user then the **Data Safe User Activity Excluded** selection will be overridden and the activity of the Data Safe service account will be audited.
   f. If you selected **All users except a specific set of users**,
   g. Click **Save**.
8. Click **Provision**.

   The selected audit policies are enabled on your target database.

> **Note:**
>
> You cannot provision a custom audit policy.

Retrieve the Latest Audit Policies for a Target Database

You can retrieve the latest audit policies for a target database at any time. This is helpful if new custom policies were added to your target database and you want to enable or disable them

through Oracle Data Safe. Or, if audit policies were provisioned from a REST API or SDK CLI, you can retrieve the policies in Oracle Data Safe to view which ones are enabled.

For database version-related limitations, please see Supported Target Databases.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Policies**.
3. On the right, click the name of your target database.

   The **Audit Policies Details** page is displayed.
4. Click **Retrieve**.

   The list of audit policies is updated on the page.

Update Users and Roles for Audit Policies

From the audit policy page for a target database, you can update the users and roles configured for provisioned audit policies.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Policies**.
3. On the right, click the name of your target database.

   The **Audit Policies Details** page is displayed.
4. For the audit policy that you want to configure users, click **View Details**.

   The **Configure Policy** panel is displayed.
5. (Optional) If the roles on the target database have been updated since the stated time and date, click **Refresh Database Roles**.
6. Select one of the following options. All three options may not be available for every audit policy.
   - **All users**
   - **Only a specific set of users and/or roles**
   - **All users except a specific set of users**
7. If you selected **All users**, then for **Audit when operations**, select **Success**, **Failure**, or **Success or Failure**.
8. If you selected **Only a specific set of users and/or roles**, click **Add Users/Roles**, and then do the following in the **Inclusion Criteria** section:
   a. From the first drop-down list, select **Users or Roles**.
   b. From the second drop-down list, select users or roles (one at a time).
   c. From the third drop-down list, select an operation status (**Success**, **Failure**, or **Success or Failure**).
   d. Click **Add**.
   e. Repeat steps a through d to add additional users and/or roles.
9. If you selected **All users except a specific set of users**, and then do the following in the **Exclusion Criteria** section:
   a. From the first drop-down list, select users to exclude (one at a time).

b. From the second drop-down list, select an operation status (**Success**, **Failure**, or **Success or Failure**).

10. Click **Update and Provision**.

Move an Audit Policy to a Different Compartment

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit policies**.
3. On the right, click the name of your target database.

   The **Audit policy information** page is displayed.
4. Click **Move resource**.

   The **Move resource** dialog box is displayed.
5. From the drop-down list, select a destination compartment.
6. Click **Move resource**.

   The audit policy is immediately moved to the specified compartment.

Add Tags for an Audit Policy

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Policies**.
3. On the right, click the name of your target database.

   The **Audit Policies Details** page is displayed.
4. Click **Add Tags**.

   The **Add Tags** dialog box is displayed.
5. Configure one or more tags, and then click **Add Tags**.

Analyze Audit Events on the Activity Auditing Dashboard

You can view and analyze auditing activity from the Activity Auditing dashboard. By default, the dashboard shows you audit events for the past one week.

View and Filter the Activity Auditing Dashboard

You can filter data displayed on the Activity Auditing dashboard by compartment, time period, and/or target database.

1. Under **Security Center**, click **Activity Auditing**.

   The **Activity Auditing** dashboard is displayed.
2. From the **Compartment** drop-down list, select the compartment that contains the target databases for which you want to view audit events. Optionally, you can select **Include child compartments**.
3. From the **Time Period** drop-down list, select the time period for the audit events.

You can select **Last 24 Hours**, **Last 1 Week**, **Last 1 Month**, **Last 3 Months**, **Last 6 Months**, or **Date Range**.

If you select **Date Range**, specify the beginning (**Time From Month**) and end (**Time To Month**) months.

4. From the **Target Databases** drop-down list, select a specific target database or **All**.

   Only target databases that are contained in the compartment (and child compartments if you selected the option) are listed.

   If you select **All**, then data for all target databases in the selected compartment is included in the dashboard.

   As you enter the name of a target database, the list of target database names is filtered.

5. View the **Failed Login Activity**, **Admin Activity**, and **All Activity** charts.
6. View the **Events Summary** and **Targets Summary** tabs.

Analyze Audit Event Data

1. Under **Security Center**, click **Activity Auditing**.

   The **Activity Auditing** dashboard is displayed.

2. Filter the dashboard as needed.
3. To view more detail for an audit event, on the **Events Summary** tab, click an event category.

   The **Event Category** page is displayed showing you a report for the audit event.

4. To view more detail for a target database, on the **Targets Summary** tab, click a target database.
5. At the top of the page, view the filters that are currently applied to the data.

   These filters are the same as those that were applied to the dashboard.

   You can modify, remove, and add filters as needed.

6. View the summary totals.
7. To view the target database names, click **Targets**.

   A **Targets** dialog box is displayed listing the target database names. Click **Close** to close the dialog box.

8. To filter the data in the table below the summary totals, click on any of the other summary totals and set a filter.
9. In the table at the bottom of the page, view the list of audit events.
10. To add and remove columns from the audit events list, from the **Actions** menu, select **Manage Columns**. The **Manage Columns** screen is displayed. Select/deselect columns, and then click **Save Changes**.

    The following columns are available:

    - Target
    - Target Type
    - Target Class
    - Location

- DB User
- Unified Audit Policies
- OS User
- Client Host
- Client IP
- Client Program
- Client ID
- Terminal
- Event
- Operation
- Object
- Object Type
- Object Owner
- Operation Status
- Error Code
- Error message
- Operation Time
- Event Fetch Time
- SQL Text
- SQL Param
- Additional SQL
- Audit Type

View and Manage Audit Reports

You can view and schedule audit reports, set filters and modify columns in audit reports, download audit reports as PDF, XLS, or JSON files, as well as create, update, and delete custom audit reports.

View a Predefined or Custom Audit Report

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit reports**.

   The **Audit reports** page is displayed, showing you a list of standard audit reports.
3. To view a predefined audit report, on the **Predefined reports** tab, click the report name that you want to view.

   The predefined report is displayed.
4. To view a custom audit report, click the **Custom Reports** tab. In the **Report Name** column, click the name of your custom report.

   Your custom report is displayed.

5. View totals in the report.

   The report totals are clickable. Some of them show you a list and some of them toggle a filter in the list of audit events. For example, if you click the total for **DB Users**, a dialog box is displayed showing you the list of database user names. Click **Close** to close the dialog box.

   Each report has its own set of total values.

6. View individual audit events in the report.

   By default, Oracle Data Safe shows the audit data for the past one week in a predefined audit report.

7. To view more detail for a particular event, click the down arrow to expand the row and show details for the particular event.

   For some details, you can copy their values to the clipboard.

> **Note:**
>
> If the audit report takes longer to process, the report is being generated in the background. You can remain on this page and wait for the report to generate, or navigate to the **Audit Report History** page, where a link to the report in JSON format will be available. For more information, see View Audit Report History.

Modifying Columns in an Audit Report

To add or remove columns in the report, do the following:

1. View a predefined or custom audit report.
2. Click **Manage Columns**.
   The **Manage Columns** window is displayed.
3. Select columns that you want displayed in the report.
4. Deselect columns that you want to hide in the report.
5. Click **Apply Changes**.

Basic Filtering in an Audit Report

To apply basic filters in the report, do the following:

1. View a predefined or custom audit report.
2. Click **Another Filter**.
3. Select a filter type, operator, and enter a value. All columns that are available in the report are available as filter types.
4. Click **Apply**.
5. Repeat steps two through four to apply additional filters.

To remove a filter, click the **X** beside the filter row.

To filter the report based on a total category (for example, Login Successes), click the total. The list of audit events in the table at the bottom of the report is automatically updated. To remove the filter, click the total again.

> **Note:**
>
> Only some totals in your report are single-click filters

Advanced Filtering in an Audit Report

Advanced filtering of audit data can provide flexibility in the way that data is analyzed and reviewed, by allowing organizations to specify complex conditions and multiple criteria that must be met in order for data to be included or excluded from the analysis.

To apply advanced filters in the report, do the following:

1. View a predefined or custom audit report.
2. Click **Show Advanced SCIM Query Builder**.
3. Use the provided filter builder and dropdowns to type in your filter(s). Advanced filtering uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:
   - `co`: matches resources with an attribute that contains a given string
   - `eq`: matches resources with an attribute that is equal to a given value (not case sensitive)
   - `eq_cs`: matches resources with an attribute that is equal to a given value (case sensitive)
   - `ew`: matches resources with an attribute that ends with a given string
   - `ge`: matches resources with an attribute that is greater than or equal to a given value
   - `gt`: matches resources with an attribute that is greater than a given value
   - `in`: matches resources with an attribute that is equal to any of given values in list
   - `le`: matches resources with an attribute that is less than or equal to a given value
   - `lt`: matches resources with an attribute that is less than a given value
   - `ne`: matches resources with an attribute that is not equal to a given value
   - `not_in` : matches resources with an attribute that is not equal to any of given values in list
   - `pr`: matches resources with an attribute if it has a given value
   - `sw`: matches resources with an attribute that starts with a given string

   Operators can be grouped using parentheses to specify the order.

   Filters can also be combined using logical operators such as `and` and `or`.

   > **Note:**
   >
   > If you have any basic filters currently applied they will appear in the query builder as well.

4. Click **Apply**.

To clear the query builder, click **Clear**. This will clear any basic filters applied as well.

Example 4-1 Failed login advanced filter

```
((operation eq "LOGIN" OR operation eq "LOGON") and operationStatus eq
"FAILURE")
```

Example 4-2 User creation or modification advanced filter

```
(operation eq "CREATE" OR operation eq "DROP" OR operation eq "ALTER") AND
(objectType
      eq "USER")
```

Example 4-3 Changes in audit policy advanced filter

```
(operation eq "AUDIT") OR (operation eq "NOAUDIT") OR (operation eq "CREATE"
AND
      objectType eq "AUDIT POLICY") OR (operation eq "ALTER" AND objectType
eq "AUDIT POLICY")
      OR (operation eq "DROP" AND objectType eq "AUDIT POLICY") OR (operation
eq "EXECUTE" AND
      objectName eq "DBMS_FGA")
```

Tips for Using the Filter Builder to Create Advanced Filters

- Pressing the escape key while in advanced filtering mode will clear the whole query.
- Pressing the space key will display the drop down with the list of available attributes or operators.
- Pressing the space key after entering a value like `targetname (demo_tgt)` will enclose the string with quotes: `("demo_tgt")`.
- Pressing enter will close the drop down listing the operators and attribute names.
- If a value like alert name has spaces in it, typing space will enclose the first word within quotes, `"alert name"`. You will have to move the cursor back to the enclosed string and continue typing the rest of the string value.
- If you build a filter in advanced filtering that can't be displayed in basic filters, you can't switch back to basic filtering mode. For example, advanced filters with the or condition can't be displayed in basic filtering.
- A custom report with basic filter can be updated with advanced filter and saved.

For more information about SCIM, see the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644.

For more information about filtering in SCIM, see the filtering section of the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644#section-3.4.2.2.

Use Audit Reports to Create Custom Alerts

You can leverage the convenience of Audit reports to create custom alert policy. Apply the filters in the All Activity report to narrow down the conditions for alerting and create a new custom alert policy or add a rule to an existing custom alert policy based on the filtered conditions.

Related Topics

- Create and Manage Custom Alert Policies
  Expand the capabilities of Data Safe Alerts by creating custom alert policies.

Create a Custom Alert Policy From the All Activity Audit Report

You can leverage the convenience of Audit reports to create custom alert policy. Apply the filters in the All Activity report to narrow down the conditions for alerting and create a new custom alert policy based on the filtered conditions.

To create a custom alert policy:

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit reports**.
3. Select the **All activity** report from the list.
4. Use basic or advanced filtering to filter the all activity report as desired for the alert policy.

> **Tip:**
>
> Don't create filters that only apply to specific target databases or times as this will cause errors when creating the policy.

   See the **Alert condition supported fields** table below for the list of valid fields.

   See Basic Filtering in an Audit Report and Advanced Filtering in an Audit Report for more information.

5. Click **Create as alert rule** to use the currently applied filters as the conditions for a custom alert.
6. Select **Create an alert policy**.
7. Fill in the following required fields:

Field Name	Description
Policy name	Display name of the alert policy you're creating.
Compartment	The compartment where the alert policy will be created. Alert policies can be applied to target databases regardless of the compartment. You will associate the alert policy to the target database in a later step. See Associate and Apply Alert Policies to Target Databases for more information.
Severity	Critical, High, Medium, or Low The designated severity level will be visible if an alert is generated.

Field Name	Description
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger. An alert policy can have up to five custom rules. You can only create one rule in this workflow, but you can create more in a later step. See Add an Alert Rule to an Existing Alert Policy From Activity Auditing or Manage the Alert Rules of an Existing Alert Policy Manually for more information.
Rule expression SCIM query	This will show the System for Cross-Domain Identity Management (SCIM) syntax for the filters you applied earlier and defines the logic for your custom alert. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

8. Click **Submit**.

Table 4-1 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.
`Client program (clientProgram)`	The application from which the audit event was generated. For example SQL Plus or SQL Developer.
`DB user (dbUserName)`	The name of the database user whose actions were audited.
`Error code (errorCode)`	Oracle Error code generated by the action. Zero indicates the action was successful.
`Error message (errorMessage)`	The detailed message on why the error occurred.
`Event (eventName)`	The name of the event executed by the user on the target database. For example `ALTER SEQUENCE`, `CREATE TRIGGER`, or `CREATE INDEX`.
`External user (externalUserId)`	The user ID of the external user of the audit event.
`Location (auditLocation)`	The location of the audit. Currently the value is audit table.
`Object(objectName)`	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, `ALTER_TABLE`.
`Object owner (objectOwner)`	The schema name of the object affected by the action.

Table 4-1 (Cont.) Alert condition supported fields

Field	Description
`Object type (objectType)`	Type of object in the source database affected by the action. For example `PL/SQL`, `SYNONYM`, or `PACKAGE BODY`.
`Operation (operation)`	The name of the action executed by the user on the target database. For example `ALTER`, `CREATE`, or `DROP`.
`Operation status (operationStatus)`	Status of the event: `Success` or `Failure`
`OS user (osUserName)`	The name of the operating system user for the database session.
`Terminal (osTerminal)`	The operating system terminal of the user session.
`Unified audit policies (auditPolicies)`	List of audit policies that caused the current audit event.

Add an Alert Rule to an Existing Alert Policy From Activity Auditing

After applying filters to the All activity report in Activity Auditing, you can add a rule to an existing custom alert policy based on the filters.

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit reports**.
3. Select the **All activity** report from the list.
4. Use basic or advanced filtering to filter the all activity report as desired for the alert policy.

   > **Tip:**
   >
   > Don't create filters that only apply to specific target databases or times as this will cause errors when creating the rule.

   See the **Alert condition supported fields** table below for the list of valid fields.

   See Basic Filtering in an Audit Report and Advanced Filtering in an Audit Report for more information.
5. Click **Create as alert rule** to use the currently applied filters as the conditions for a custom alert.
6. Select **Create as alert rule** to use the currently applied filters as the conditions for an additional rule of an existing alert policy.
   An alert policy can have up to five alert rules. The policy will trigger if any of the rules are met.
7. Fill in the following required fields:

Field Name	Description
Compartment	Select the compartment where the alert policy you're adding the rule to is stored.

Field Name	Description
Policy name	Select the name of the alert policy. The list is populated based on the compartment that is selected.
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger. An alert policy can have up to five custom rules. You can only create one rule in this workflow, but you can create more in a later step. See Add an Alert Rule to an Existing Alert Policy From Activity Auditing or Manage the Alert Rules of an Existing Alert Policy Manually for more information.
Rule expression SCIM query	This will show the System for Cross-Domain Identity Management (SCIM) syntax for the filters you applied earlier and defines the logic for your custom alert. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

8. Click **Submit**.

Table 4-2 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.
`Client program (clientProgram)`	The application from which the audit event was generated. For example SQL Plus or SQL Developer.
`DB user (dbUserName)`	The name of the database user whose actions were audited.
`Error code (errorCode)`	Oracle Error code generated by the action. Zero indicates the action was successful.
`Error message (errorMessage)`	The detailed message on why the error occurred.
`Event (eventName)`	The name of the event executed by the user on the target database. For example `ALTER SEQUENCE`, `CREATE TRIGGER`, or `CREATE INDEX`.
`External user (externalUserId)`	The user ID of the external user of the audit event.
`Location (auditLocation)`	The location of the audit. Currently the value is audit table.

Table 4-2 (Cont.) Alert condition supported fields

Field	Description
`Object(objectName)`	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, `ALTER_TABLE`.
`Object owner (objectOwner)`	The schema name of the object affected by the action.
`Object type (objectType)`	Type of object in the source database affected by the action. For example `PL/SQL`, `SYNONYM`, or `PACKAGE BODY`.
`Operation (operation)`	The name of the action executed by the user on the target database. For example `ALTER`, `CREATE`, or `DROP`.
`Operation status (operationStatus)`	Status of the event: `Success` or `Failure`
`OS user (osUserName)`	The name of the operating system user for the database session.
`Terminal (osTerminal)`	The operating system terminal of the user session.
`Unified audit policies (auditPolicies)`	List of audit policies that caused the current audit event.

Download an Audit Report

Downloading the latest report can be done from either the list of Audit Reports or the details of the audit report. In addition you can download any report from the past three months from either the Audit Report History list or the details of the scheduled or generated audit report.

Download the latest audit report from a list of Audit Reports:

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**. The **Audit Reports** page is displayed, showing you a list of standard audit reports.
3. On the **Predefined Reports** or **Custom Reports** tab, locate the row that has the report you want to download.
4. In the **Latest Report** column, click the download button (downward pointing arrow). The report is downloaded to your browser.
5. Using your browser's options, open and view the report, or save it to your local computer.

Download the latest audit report from the details page of the Audit Report:

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**. The **Audit Reports** page is displayed, showing you a list of standard audit reports.
3. Select an audit report from either the **Predefined Reports** or **Custom Reports** tab.
4. Click the **Download Report** button. The latest report will be downloaded.
5. Using your browser's options, open and view the report, or save it to your local computer.

Download an audit report from the Audit Report History list

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Report History**. The **Audit Report History** page is displayed, showing you a list of scheduled and generated audit reports from the last three months.
3. Locate the row that has the report you want to download and click the button in the **Download Report** column. The report will be downloaded.

Download an audit report from the Audit Report History details page

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Report History**. The **Audit Report History** page is displayed, showing you a list of scheduled and generated audit reports from the last three months.
3. Click on the name of an audit report from the list.
4. Click the **Download Report** button. The report will be downloaded.

Generate and Download a PDF or XLS Audit Report

You can generate and download a predefined audit report as a PDF or XLS document. You need to first generate the report before you can download it.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**.

   The **Audit Reports** page is displayed, showing you a list of standard audit reports.
3. On the **Predefined Reports** tab, click the report name for which you want to generate a PDF or XLS report.

   The report page is displayed.
4. Click **Generate Report**.

   The **Generate Report** dialog box is displayed.
5. For **Report Format**, select **PDF** or **XLS**.
6. Enter a display name for the report.
7. (Optional) Enter a report description.
8. Select a compartment in which to store your report.
9. (Optional) Set filters on the audit data as needed:
   - Specify a maximum number of rows (row limit) to display in the report. If unspecified, the default row limit is 200 rows.
   - Select specific target databases.
   - Set a report start time and end time.
10. Click **Generate Report**.

    The report is generated and saved to the specified compartment.
11. When the report is finished generating, do one of the following:

- In the **Generate Report** dialog box next to **To download report please**, click the **click here** link. A dialog box is displayed where you can specify whether you want to open or save the file.
- Click **Close** to close the **Generate Report** dialog box, and then click **Download Report**. A dialog box is displayed where you can specify whether you want to open or save the file.

Create a Custom Audit Report

You can create a custom audit report from a predefined or existing custom audit report. You may want to do this if you have specific filters set and columns displayed that you want to preserve. Or, you may want to change the filters and columns in the custom report. During creation, you can save the report to a compartment of your choice.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**.

   The **Audit Reports** page is displayed, showing you a list of standard audit reports.
3. On the **Predefined Reports** tab, click the predefined report name from which you want to create your custom report.

   The report page is displayed.
4. Click **Create Custom Report**.

   The **Custom Report** dialog box is displayed.
5. Enter a report name.
6. (Optional) Enter a report description.
7. Select the compartment to which you want to save your report.
8. Click **Create Custom Report**.

   The audit data and filters that are currently displayed on the page are saved in the custom report. The custom report is listed on the **Custom Reports** tab.

Update a Custom Audit Report

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**.
3. Click the **Custom Reports** tab.
4. In the **Report Name** column, click the name of the custom report that you want to update.

   Your custom report is displayed.
5. Modify the report as needed.
6. Click **Save Report**.

   The report is updated.

Delete a Custom Audit Report

> **Important:**
>
> Be careful when you delete a custom audit report, because you can't recover one after it's deleted.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**.
3. Click the **Custom Reports** tab.
4. In the **Report Name** column, click the name of the custom report that you want to delete.

   Your custom report is displayed.
5. Click **Delete Report**.

   The **Delete Report** dialog box is displayed.
6. Click **Delete Report** to confirm the deletion.

Schedule a Predefined or Custom Audit Report

You can create a schedule for a predefined or custom audit report to generate a PDF or XLS report.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Reports**.

   The **Audit Reports** page is displayed, showing you a list of standard audit reports.
3. To view a predefined audit report, on the **Predefined Reports** tab, in the **Report Name** column, click the report name that you want to view.

   The predefined report is displayed.
4. To view a custom audit report, click the **Custom Report** tab. In the **Report Name** column, click the name of your custom report.

   Your custom report is displayed.
5. Click **Manage Report Schedule**.

   The **Manage Report Schedule** panel is displayed, pre-loaded with either the default or modified schedule.
6. (Optional) In the **Schedule Report Name** box, enter a name for the PDF or XLS report.
7. Select a compartment to store the reports generated by the schedule.
8. For **Report Format**, select either a **PDF** or **XLS** output.
9. Select a **Schedule Frequency**.
   - If you select weekly, select the day of the week in the **Every** field.
   - If you select monthly, select the day of the month in the **Day** field.
10. In **Time (in UTC)**, select a schedule time.

11. In **Events Time Span**, select the time span for the audit records.

    For example, selecting Last Months and entering 14 pulls events from the last 14 months from the time the report is run.

12. (Optional) Specify a row limit. If unspecified, the default row limit is 200 rows.

13. Click **Save Schedule**.

    You can access the generated PDF/XLS reports on the **Audit Report History** page.

View Audit Report History

The **Audit Report History** page lists all the PDF/XLS/JSON audit reports that are automatically generated via a schedule or on-demand by users. On this page, you can view the list of reports generated during the past three months, details about those reports, and download reports. Oracle Data Safe stores PDF/XLS audit reports for up to three months and JSON format reports for up to 1 week. JSON format reports are generated when online audit report generation takes longer than expected.

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit report history**.

   The Audit report history table is displayed. It contains the following information:

   - **Report Name** - The name of the audit report.
   - **Lifecycle State** - Either ACTIVE or UPDATING, shows if the report is currently accessible or if it is being updated.
   - **Report Definition** - Specifies the name of the report that provides data for this scheduled or generated report.
   - **Generated Time** - The time the report was created.
   - **Report Type** - Generated or Scheduled. Where generated reports are on-demand reports produced outside of the scheduling system and scheduled reports are those produced by the scheduling system.
   - **File Format** - PDF, XLS, or JSON
   - **Download Report** - Option to download the report.

3. (Optional) Under **Filters**, narrow down the report history page based on the **Report definition**, **Report type**, **File format**, and **Time period**.

Move an Audit Report to a Different Compartment

Any scheduled or generated audit report from the past three months can be moved to a different compartment that you have access to from Audit Report History.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Audit Report History**.

   The Audit Report History table is displayed.

3. Click on the name of an audit report from the list.
4. Click **Move Resource**.
5. In the move resource dialog box, select the compartment to move the audit report to. You must have the appropriate `DATA_SAFE_REPORT_MOVE` permissions for the selected compartment.

6. Click **Move Resource**.

   The audit report and Archive Data Retrieval will be moved to the selected compartment immediately.

View and Manage Archived Audit Data

You can view and archive data retrieval details, retrieve and return audit data to the archive as needed, and move an audit data retrieval to a different compartment.

Archive Data Retrieval Details

Oracle Data Safe provides the following details for each archive data retrieval:

- **Retrieval name** (editable) - Name created by the user who created the archived audit data retrieval
- **Target database** - Target database for which the archived audit data applies
- **Archive data description** (editable) - Description created by the user who retrieved the archived audit data
- **Archive data OCID** - Oracle Cloud Identifier for the archive data retrieval object in Oracle Cloud Infrastructure
- **Compartment** - Compartment in which the archived audit data was saved to for the month
- **Retrieval period** - Beginning and end dates of the retrieval period
- **Expiry time** - Date and time when the archived audit data needs to be returned to the archive
- **Requested time** - Date and time when the user requested the archived audit data
- **Completed time** - Date and time when the archived data was retrieved
- **Records retrieved** - Number of audit records retrieved from the archive

View Details for an Archive Data Retrieval

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Archive Data Retrievals**. The **Archive Data Retrievals** page is displayed.
3. In the table, locate the row for the retrieval for which you want to view details, and click the target database name.

   The **Archive Data Retrieval Details** page is displayed.
4. On the **Archive Data Retrievals Details** tab, view the information.
5. To view the work requests related to the archive data retrieval, scroll down the page and view the listings under **Work Requests**.
   - For each work request, you can view its status (for example, ACCEPTED), the date/time when the work request was accepted, and the date/time when the work request was finished.
   - Click a particular work request to view its log messages and error messages. Log messages are displayed by default. To view error messages, under **Resources**, click **Error Messages**.

- (Optional) If there was a work request failure, notice the error message displayed at the top of the page.

Retrieve Audit Data from the Archive

This task brings archived audit data into the Oracle Data Safe *online* repository so that you can view the data in Activity Auditing reports. The retrieved data will be retained for one month and then automatically deleted from online storage. It can be deleted sooner than one month if you return the retrieved data, sending it back to the archive. The data will remain in the archive until the archival policy.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Archive Data Retrievals**.

   The **Archive Data Retrievals** page is displayed. For each listing in the table, you can view the target database, retrieval name, retrieval period (begin and end date), number of audit records retrieved, date/time when the audit data was retrieved, and date/time when the retrieval period expires.
3. Click **Retrieve Data**.

   The **Retrieve Archive Data** page is displayed.
4. For **Target Databases**, one at a time, select the target databases for which you want to retrieve archive audit data.
5. For **Display name for Archive Data**, leave the default name as is or enter a name.
6. (Optional) For **Description**, enter a brief explanation.

   For example, you may want to state the reason for retrieving the archive data.
7. For **Compartment**, select the compartment to which you want to save the retrieved audit data.
8. For **Start Month**, click the box and select a start date for the audit data.
9. For **End Month**, click the box and select an end date for the audit data.
10. Click **Retrieve**.

    A new entry is added to the table on the **Archive Data Retrievals** page.

Related Topics

- Return Audit Data to the Archive

Return Audit Data to the Archive

Prior to the expiry of retrieved audit data, you can choose to drop the data from the online repository and return it to the archive. Oracle Data Safe deletes the retrieval resource and the audit data becomes unavailable in the reports.

1. Under **Security Center**, click **Activity Auditing**.
2. Under **Related Resources**, click **Archive Data Retrievals**.

   The **Archive Data Retrievals** page is displayed.
3. In the table, locate the row for the retrieval resource that you want to return to the archive.

   The **Archive Data Retrieval Details** page is displayed.

4. Click **Release**.

   The **Release Data to Archive** dialog box is displayed asking you to confirm that you want to delete the audit archive retrieval resource.

5. Click **Release Data to Archive**.

   The retrieval resource is removed from the table on the **Archive Data Retrievals** page. The audit data is returned to the archive and can be retrieved again if needed.

Move an Archive Data Retrieval

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Archive data retrievals**.

   The **Archive data retrievals** page is displayed.

3. In the table, locate the row for the retrieval resource that you want to move, and click the target database name.

   The **Archive data retrieval information** page is displayed.

4. Click **Move resource**.

   The **Move resource** dialog box is displayed.

5. From the drop-down list, select a destination compartment.
6. Click **Move resource**.

   The retrieval resource is moved immediately.

Create and Modify Event Notifications in Activity Auditing

You can create and modify event notifications in Activity Auditing.

Creating Event Notifications for Activity Auditing

In Data Safe you can create event notifications for Activity Auditing related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **Activity auditing**.
2. You can either
   - Click the **Notifications** tab on the dashboard to create event notifications for any Activity Auditing Event or
   - Under **Related resources**, click **Audit profiles**, **Audit policies**, **Audit trails**, **Archive data retrievals**, or **Audit reports** to create specific event notifications. Once at the desired page, click the **Notifications** tab.

3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   Optionally, click on **+ Another condition** to add an additional condition to the rule.

   a. Select a **Condition**.
      If you selected **Attribute** in the previous step, select an **Attribute name** and **Attribute values**.

      If you selected **Filter tag** in the previous step, select a **Tag namespace**, a **Tag key**, and a **Tag value**.

   See Activity Auditing Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

   > **Note:**
   >
   > This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
12. Click **Create notification**.

Modifying Event Notifications For Activity Auditing

After creating event notifications in Activity Auditing in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **Activity auditing**.
2. You can either
   - Click the **Notifications** tab on the dashboard to modify event notifications for any Activity Auditing Event or
   - Under **Related resources**, click **Audit profiles**, **Audit policies**, **Audit trails**, **Archive data retrievals**, or **Audit reports** to modify specific event notifications. Once at the desired page, click the **Notifications** tab.
3. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

4. Click on **Edit Rule** to modify the event and rule.
5. You can modify the **Display Name**, **Description**, **Rule Conditions**, and **Actions** as needed.
6. Click **Save changes**.

To modify the topic and subscription:

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit profiles**, **Audit policies**, **Audit trails**, **Archive data retrievals**, or **Audit reports** based on what subscription you'd like to modify up.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

5
Alerts

This section discusses how to generate alerts based on audit events in Oracle Data Safe.

Alerts Overview

You can enable alerts on your target databases to track and be notified of particular user activities and unusual behavior.

You can choose to be alerted when a database parameter or audit policy changes, a failed login by an admin occurs, a user entitlement changes, and when a user is created or deleted.

About Alerts in Oracle Data Safe

An alert message proactively notifies you when a particular audit event happens on a target database. Alerts are based on the alert policies that you enable in Oracle Data Safe.

As a prerequisite to alert notification, you need an enabled audit policy. This policy is what generates the audit event. If the generated audit event matches the alert policy enabled for the target database, an alert is raised.

Oracle Data Safe Alert Policies

In Security Center, you can provision custom and predefined alert policies on your target databases. An alert policy defines a database event to monitor. Alert policies are rule-based and are triggered from the audit data collected. Alerts have a retention policy of 3 months by default.

For example, if the `ORA_LOGON_FAILURES` unified audit policy is provisioned on the target database, then when an administrator fails to login to the target database, a Failed login audit record is generated because of this policy. The generated audit record is collected by Oracle Data Safe. When the alert policy `Failed Logins by Admin User` is enabled for the target, an alert is raised by Oracle Data Safe for the Failed login audit record.

Custom Alerts

Custom alert policies allow you to customize what database changes you'd like to be alerted about. Possible scenarios that you can configure alerts for include:

- Detect database parameter changes from unknown client hosts
- Detect data access on important tables from non allow-listed users
- Detect changes of stored procedure definition to execute unwanted logic
- Detect Database Vault realm violations on sensitive application schema
- Detect data exfiltration attempts from sensitive tables

See Create and Manage Custom Alert Policies for more information.

Pre-defined Alerts

The following table lists the Oracle predefined alert policies, their severity levels, their descriptions, and the basis for each alert.

Predefined Alert	Severity Level	Description	Required audit policies to trigger alert
Audit policy changes	High	Modifications to audit policies such as `CREATE`, `ALTER`, `DROP`, `AUDIT`, and `NOAUDIT`, as well as executions of `DBMS_AUDIT_MGMT` or `DBMS_FGA` package	These are captured by mandatory audits in an Oracle Database.
Database parameter changes	High	Changes to database parameters using `ALTER SYSTEM` statement	Critical Database Activity or `ORA_DATABASE_PARAMETER` audit policy
Database schema changes	Medium	Any changes to Data Definition Language (DDL) actions such as `CREATE`, `ALTER`, `DROP`, or `TRUNCATE` on database schema objects*	Database Schema Changes or a similar audit policy
Failed logins by admin user	Critical	All failed login attempts by an admin user who has either administrative or system privileges	`ORA_LOGIN_FAILURES` (`ORA_LOGIN_LOGOUT` for 23ai) or a similar policy
Profile changes	Critical	Any changes to user profiles such as `CREATE`, `ALTER`, or `DROP`	Critical Database Activity or a similar audit policy
User creation/ modification	Medium	Any changes to database users such as `CREATE`, `ALTER`, or `DROP`	Critical Database Activity, `ORA_ACCOUNT_MGMT`, or a similar policy
User entitlement changes	Medium	Any changes to user entitlement data such as `GRANT` or `REVOKE` of privileges on any database objects	Critical Database Activity, `ORA_ACCOUNT_MGMT`, or a similar policy
SQL Firewall violations	Critical	SQL Firewall logs violations in real-time for every unmatched scenario of database connection or SQL command execution against the entries in the enabled allowlist rules of the SQL Firewall policy.	Enable audit when you deploy and enforce SQL Firewall policy for the database user

*Database schema objects include: `PROCEDURE`, `PACKAGE`, `PACKAGE BODY`, `FUNCTION`, `TRIGGER`, `LIBRARY`, `SYNONYM`, `TABLE`, `DATABASE LINK`, `INDEX`, `OUTLINE`, `CONTEXT`, `ATTRIBUTE DIMENSION`, `DIMENSION`, `INDEXTYPE`, `OPERATOR`, `JAVA`, `MINING MODEL`, `TYPE BODY`, `TYPE`, `MATERIALIZED VIEW`, `MATERIALIZED VIEW LOG`, `MATERIALIZED ZONEMAP`, `VIEW`, `ANALYTIC VIEW`, `SEQUENCE`, and `CLUSTER`

Target-Policy Associations

When you apply an alert policy on a target database, Oracle Data Safe creates an association between your target database and the alert policy, and automatically enables the policy on your target database. You can view associations on the **Target-Policy Associations** page in Security Center. You can disable or re-enable the alert policy as needed and delete the target-policy association. Disabling the alert policy does not pause audit collection. It temporarily pauses the policy evaluation for the audit event.

This is the typical use case. During a maintenance window, you know that certain activities in the database are going to generate audit events, but you do not want alert notifications sent to the administrator during this window. You can pause the alert evaluation by disabling it momentarily.

> **Important:**
>
> You can apply alert policies before or after audit data collection is started for a target database. But when you want to start generating alerts, first ensure that appropriate audit polices are configured, that audit collection is enabled for the audit trails, and that Oracle Data Safe is collecting audit data from the target database.

Throttled Alerts

Custom and predefined alert policies will automatically be throttled, temporarily paused, by Data Safe if 1000 or more alerts are generated within a ten minute interval.

In order to prevent an overwhelming amount of alerts that can occur due to improper configuration of audit or alert policies or due to changes in the application workload generating the audit events, Data Safe will throttle, temporarily pause, an alert policy if it generates 1000 or more alerts based on the audit collection data from one audit trail on a target database within a ten minute interval. These ten minute intervals have been designated by Data Safe as every ten minutes starting from the top of the hour.

If an alert policy is throttled, you will receive an **Alert Generation Throttled** alert informing you of the alert policy that has been throttled. When an alert policy is throttled, it is temporarily paused for up to ten minutes, for the remainder of the same ten-minute interval that the alerts were generated in, to allow you time to analyze if this abnormal volume of alerts is because of account misconfigurations in audit or alert policies or indicative of a potential breach. Once throttling is complete at the end of the ten minute interval, the alert policy will be enabled again.

For example, if an alert policy causes over 1000 alerts between 08:03 and 08:07, then you will receive the **Alert Generation Throttled** alert at 8:07 and the alert will be throttled until 08:09:59 as 08:00:00 to 08:09:59 is a designated ten minute interval. However, if an alert policy causes 501 alerts between 08:05 and 08:09:59 and additionally 501 alerts between 08:10 and 08:15, assuming no other alerts, the alert policy will not throttle as neither the 08:00:00 to 08:09:59 nor the 08:10:00 to 08:19:59 interval had 1000 or more alerts.

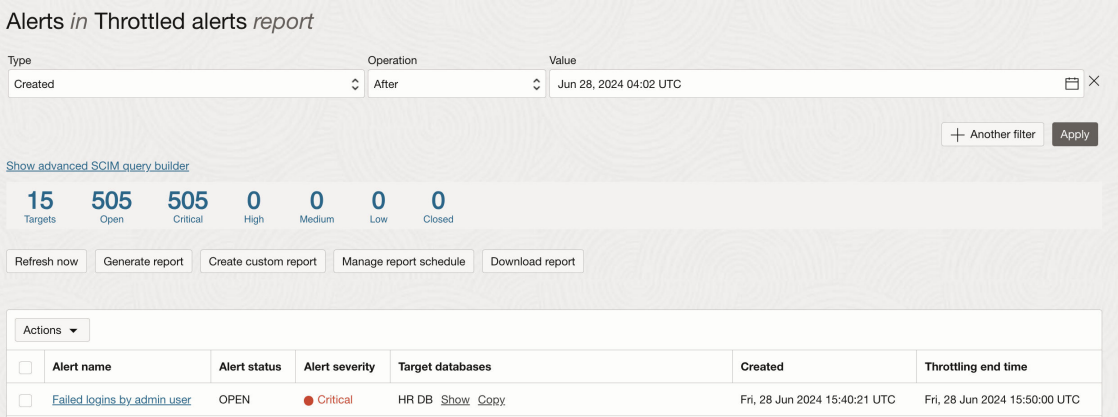
Because alert policies are evaluated at the time of audit collection in Data Safe, it is possible that the actual audit event was generated in the target database in the past. For instance, if you start an audit trail collection for a newly registered database to bring in a year's worth of audit data, Data Safe will evaluate the alert policies based on the collected audit data that is a year old and will throttle a alert policy if it generates 1000 or more alerts within a ten minute interval while parsing through the audit data. More specifically, if parsing through six hours of past audit data takes Data Safe from 10:02 to 10:07, and over 1000 alerts were triggered for an alert policy, then that alert policy will be throttled until 10:09:59.

Throttled Alerts Report

You can see more details about the throttled alert policies in the **Throttled alerts** report which is available in the **Reports** related resource. In addition to general information for the throttled alerts you will see these columns:

- **Created**: The time when the alert policy was first throttled.
- **Throttling end time**: The time when the alert policy was done being throttled.

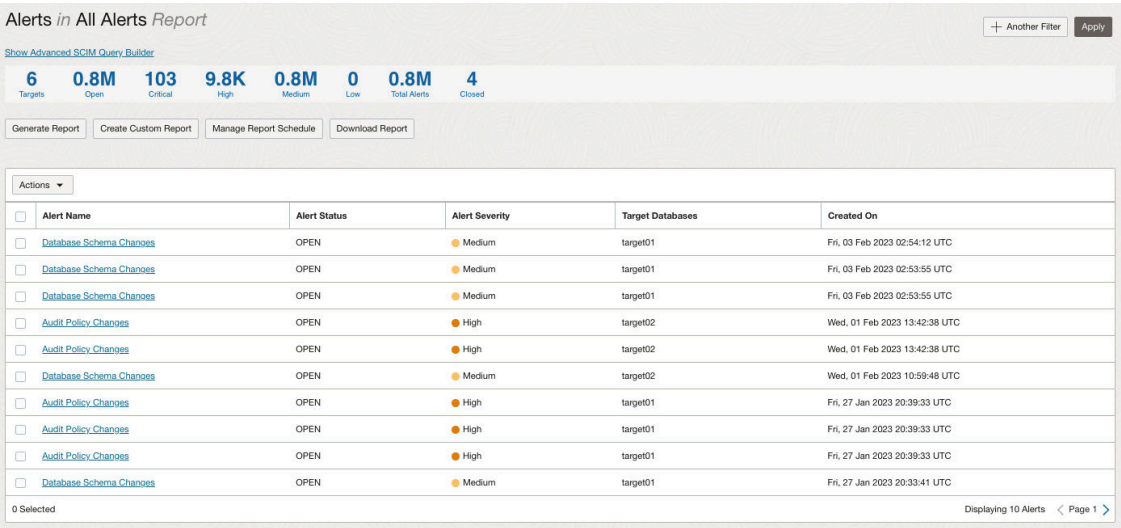
Figure 5-1 Throttled alerts report example



See View and Manage Alert Reports for more information.

All Alerts Report

Oracle Data Safe provides an interactive All Alerts report that shows you a high-level summary of your alerts. You can set filters, show and hide report columns, save your changes as a custom report, and generate and download PDF and XLS reports. You can update, delete, and generate PDF and XLS reports from custom reports. You cannot delete the All Alerts report. The following screenshot shows you an example of an All Alerts report for six target databases.



Alerts Workflow

The general steps for applying for a target database are as follows:

1. Obtain permissions in Oracle Cloud Infrastructure Identity and Access Management (IAM) to inspect target databases and use the Alerts feature in the relevant compartment.
2. Register your target database. A default audit profile, audit policy, and audit trail are automatically created for you.
3. Review and modify the default audit profile for your target database to customize audit data retention settings and paid usage settings.
4. Review and modify the default audit policy for your target database to ensure the unified audit policies that are appropriate to track activities of interest are enabled on your target database. Among those policies, decide which audit events you want to configure for proactive monitoring via alerts.
5. Review the audit trails for your target database **and ensure that they are started** so that they can collect audit data. They should be in either the Collecting or Idle state.
6. Create custom alert policies.
7. Apply alert policies to your target database.
   - When an alert policy is enabled, you can receive alerts for that policy.
   - When an alert policy is disabled, alert policy evaluation is suspended. Audit policy and audit data collection remains intact.
8. Set up event and alarm notifications. For example, you can subscribe to the `Alert Generated` event to be automatically informed when an alert is generated. Additionally, you can set up an alarm to receive a notification when for example, over a 100 alerts are generated within 5 minutes.

Prerequisites for Using Alerts

These are the prerequisites for using Alerts:

- **Register the target databases that you want to use with the Alerts feature.**
- **Obtain permission in Oracle Cloud Infrastructure Identity and Access Management (IAM) to use the Alerts feature in Oracle Data Safe.** An OCI administrator can grant `view` or `manage` permission as needed on the following resources::
  - `data-safe-alerts`
  - `data-safe-alert-policies`
  - `data-safe-target-alert-policy-associations`
  - `data-safe-report-definitions`
  - `data-safe-work-requests` (lets you view the list of work requests and their details)

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-alert-family` in the relevant compartments, which would include permissions on all of the resources above. See data-safe-alert-family Resource in the *Administering Oracle Data Safe* guide for more information.

> **See Also:**
>
> The *Administering Oracle Data Safe* guide provides these sections to help with establishing the prerequisites:
>
> - Migrate to Oracle Cloud Infrastructure You can follow the one-time migration procedure described in the guide or you can do the migration manually.
> - Grant Roles to the Oracle Data Safe Service Account on Your Target Database describes the roles required for Activity Auditing and for other Oracle Data Safe features.
> - Create IAM Policies for Oracle Data Safe describes the privileges required for each feature in Oracle Data Safe.

View and Manage Alert Policies

You can view and perform management tasks with alert policies.

Create and Manage Custom Alert Policies

Expand the capabilities of Data Safe Alerts by creating custom alert policies.

Related Topics

- Throttled Alerts
  Custom and predefined alert policies will automatically be throttled, temporarily paused, by Data Safe if 1000 or more alerts are generated within a ten minute interval.

Create a Custom Alert Policy From the All Activity Audit Report

You can leverage the convenience of Audit reports to create custom alert policy. Apply the filters in the All Activity report to narrow down the conditions for alerting and create a new custom alert policy based on the filtered conditions.

To create a custom alert policy:

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit reports**.
3. Select the **All activity** report from the list.
4. Use basic or advanced filtering to filter the all activity report as desired for the alert policy.

> **Tip:**
>
> Don't create filters that only apply to specific target databases or times as this will cause errors when creating the policy.

See the **Alert condition supported fields** table below for the list of valid fields.

See Basic Filtering in an Audit Report and Advanced Filtering in an Audit Report for more information.

5. Click **Create as alert rule** to use the currently applied filters as the conditions for a custom alert.
6. Select **Create an alert policy**.
7. Fill in the following required fields:

Field Name	Description
Policy name	Display name of the alert policy you're creating.
Compartment	The compartment where the alert policy will be created. Alert policies can be applied to target databases regardless of the compartment. You will associate the alert policy to the target database in a later step. See Associate and Apply Alert Policies to Target Databases for more information.
Severity	Critical, High, Medium, or Low The designated severity level will be visible if an alert is generated.
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger. An alert policy can have up to five custom rules. You can only create one rule in this workflow, but you can create more in a later step. See Add an Alert Rule to an Existing Alert Policy From Activity Auditing or Manage the Alert Rules of an Existing Alert Policy Manually for more information.
Rule expression SCIM query	This will show the System for Cross-Domain Identity Management (SCIM) syntax for the filters you applied earlier and defines the logic for your custom alert. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

8. Click **Submit**.

Table 5-1 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.
`Client program (clientProgram)`	The application from which the audit event was generated. For example SQL Plus or SQL Developer.

Table 5-1 (Cont.) Alert condition supported fields

Field	Description
DB user (dbUserName)	The name of the database user whose actions were audited.
Error code (errorCode)	Oracle Error code generated by the action. Zero indicates the action was successful.
Error message (errorMessage)	The detailed message on why the error occurred.
Event (eventName)	The name of the event executed by the user on the target database. For example ALTER SEQUENCE, CREATE TRIGGER, or CREATE INDEX.
External user (externalUserId)	The user ID of the external user of the audit event.
Location (auditLocation)	The location of the audit. Currently the value is audit table.
Object(objectName)	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, ALTER_TABLE.
Object owner (objectOwner)	The schema name of the object affected by the action.
Object type (objectType)	Type of object in the source database affected by the action. For example PL/SQL, SYNONYM, or PACKAGE BODY.
Operation (operation)	The name of the action executed by the user on the target database. For example ALTER, CREATE, or DROP.
Operation status (operationStatus)	Status of the event: Success or Failure
OS user (osUserName)	The name of the operating system user for the database session.
Terminal (osTerminal)	The operating system terminal of the user session.
Unified audit policies (auditPolicies)	List of audit policies that caused the current audit event.

Create a Custom Alert Policy Manually

You can use System for Cross-Domain Identity Management (SCIM) syntax to create custom alert policies. Existing alert policies can be used as the basis for a custom alert policy and further customized using SCIM.

To create a custom alert policy:

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Alert policies**.
3. Click **Create alert policy**.
4. Fill in the following required fields:

Field Name	Description
Policy name	Display name of the alert policy you're creating.

Field Name	Description
Compartment	The compartment where the alert policy will be created. Alert policies can be applied to target databases regardless of the compartment. You will associate the alert policy to the target database in a later step. See Associate and Apply Alert Policies to Target Databases for more information.
Severity	Critical, High, Medium, or Low The designated severity level will be visible if an alert is generated.
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger. An alert policy can have up to five custom rules. You can only create one rule in this workflow, but you can create more in a later step. See Add an Alert Rule to an Existing Alert Policy From Activity Auditing or Manage the Alert Rules of an Existing Alert Policy Manually for more information.
Rule expression SCIM query	Use System for Cross-Domain Identity Management (SCIM) syntax to create the logic that will cause the alert to trigger. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. **Tip:** Don't create rules that only apply to specific target databases or times as this will cause errors. See the **Alert condition supported fields** table below for the list of valid fields. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

5. Click **Submit**.

Table 5-2 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.

Table 5-2 (Cont.) Alert condition supported fields

Field	Description
Client program (clientProgram)	The application from which the audit event was generated. For example SQL Plus or SQL Developer.
DB user (dbUserName)	The name of the database user whose actions were audited.
Error code (errorCode)	Oracle Error code generated by the action. Zero indicates the action was successful.
Error message (errorMessage)	The detailed message on why the error occurred.
Event (eventName)	The name of the event executed by the user on the target database. For example ALTER SEQUENCE, CREATE TRIGGER, or CREATE INDEX.
External user (externalUserId)	The user ID of the external user of the audit event.
Location (auditLocation)	The location of the audit. Currently the value is audit table.
Object(objectName)	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, ALTER_TABLE.
Object owner (objectOwner)	The schema name of the object affected by the action.
Object type (objectType)	Type of object in the source database affected by the action. For example PL/SQL, SYNONYM, or PACKAGE BODY.
Operation (operation)	The name of the action executed by the user on the target database. For example ALTER, CREATE, or DROP.
Operation status (operationStatus)	Status of the event: Success or Failure
OS user (osUserName)	The name of the operating system user for the database session.
Terminal (osTerminal)	The operating system terminal of the user session.
Unified audit policies (auditPolicies)	List of audit policies that caused the current audit event.

Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM)

Use the following information to use SCIM to create custom alert policies.

Supported SCIM Operators

Rule expression creation uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:

- co: matches resources with an attribute that contains a given string
- eq: matches resources with an attribute that is equal to a given value (not case sensitive)
- eq_cs: matches resources with an attribute that is equal to a given value (case sensitive)
- ew: matches resources with an attribute that ends with a given string

- `ge`: matches resources with an attribute that is greater than or equal to a given value
- `gt`: matches resources with an attribute that is greater than a given value
- `in`: matches resources with an attribute that is equal to any of given values in list
- `le`: matches resources with an attribute that is less than or equal to a given value
- `lt`: matches resources with an attribute that is less than a given value
- `ne`: matches resources with an attribute that is not equal to a given value
- `not_in` : matches resources with an attribute that is not equal to any of given values in list
- `pr`: matches resources with an attribute if it has a given value
- `sw`: matches resources with an attribute that starts with a given string

Tips for Using SCIM

- Pressing the escape key while defining the rule expression will clear the whole query and close the create alert policy workflow.
- Pressing the space key will display the drop down with the list of available attributes or operators.
- Pressing the space key after entering a value like `objectName (demo_obj)` will enclose the string with quotes: `("demo_obj")`.
- Pressing enter will close the drop down listing the operators and attribute names.
- If a value like SQL Firewall policy name has spaces in it, typing space will enclose the first word within quotes, `"policy name"`. You will have to move the cursor back to the enclosed string and continue typing the rest of the string value.

For more information about SCIM, see the protocol documentation at https://www.rfceditor.org/rfc/rfc7644.

For more information about filtering in SCIM, see the filtering section of the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644#section-3.4.2.2.

Add an Alert Rule to an Existing Alert Policy From Activity Auditing

After applying filters to the All activity report in Activity Auditing, you can add a rule to an existing custom alert policy based on the filters.

1. Under **Security center**, click **Activity auditing**.
2. Under **Related resources**, click **Audit reports**.
3. Select the **All activity** report from the list.
4. Use basic or advanced filtering to filter the all activity report as desired for the alert policy.

> **Tip:**
>
> Don't create filters that only apply to specific target databases or times as this will cause errors when creating the rule.

See the **Alert condition supported fields** table below for the list of valid fields.

See Basic Filtering in an Audit Report and Advanced Filtering in an Audit Report for more information.

5. Click **Create as alert rule** to use the currently applied filters as the conditions for a custom alert.
6. Select **Create as alert rule** to use the currently applied filters as the conditions for an additional rule of an existing alert policy.
   An alert policy can have up to five alert rules. The policy will trigger if any of the rules are met.
7. Fill in the following required fields:

Field Name	Description
Compartment	Select the compartment where the alert policy you're adding the rule to is stored.
Policy name	Select the name of the alert policy. The list is populated based on the compartment that is selected.
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger. An alert policy can have up to five custom rules. You can only create one rule in this workflow, but you can create more in a later step. See Add an Alert Rule to an Existing Alert Policy From Activity Auditing or Manage the Alert Rules of an Existing Alert Policy Manually for more information.
Rule expression SCIM query	This will show the System for Cross-Domain Identity Management (SCIM) syntax for the filters you applied earlier and defines the logic for your custom alert. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

8. Click **Submit**.

Table 5-3 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.
`Client program (clientProgram)`	The application from which the audit event was generated. For example SQL Plus or SQL Developer.
`DB user (dbUserName)`	The name of the database user whose actions were audited.
`Error code (errorCode)`	Oracle Error code generated by the action. Zero indicates the action was successful.

Table 5-3 (Cont.) Alert condition supported fields

Field	Description
Error message (errorMessage)	The detailed message on why the error occurred.
Event (eventName)	The name of the event executed by the user on the target database. For example ALTER SEQUENCE, CREATE TRIGGER, or CREATE INDEX.
External user (externalUserId)	The user ID of the external user of the audit event.
Location (auditLocation)	The location of the audit. Currently the value is audit table.
Object(objectName)	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, ALTER_TABLE.
Object owner (objectOwner)	The schema name of the object affected by the action.
Object type (objectType)	Type of object in the source database affected by the action. For example PL/SQL, SYNONYM, or PACKAGE BODY.
Operation (operation)	The name of the action executed by the user on the target database. For example ALTER, CREATE, or DROP.
Operation status (operationStatus)	Status of the event: Success or Failure
OS user (osUserName)	The name of the operating system user for the database session.
Terminal (osTerminal)	The operating system terminal of the user session.
Unified audit policies (auditPolicies)	List of audit policies that caused the current audit event.

Manage the Alert Rules of an Existing Alert Policy Manually

After creating a custom alert policy you can add up to four additional custom alert rules, up to five rules total, to an existing custom alert policy. An alert will be triggered if any of the alert rules are met.

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Alert policies**.
3. Click the **Custom alert policies** tab.
4. Select the custom alert policy you'd like mange the alert rules for.
5. You can perform the following tasks:
   - Click **Add rule** to add a new rule. Enter the required fields as described in the following table.
     An alert policy can have up to five alert rules. The policy will trigger if any of the rules are met
   - Select an existing rule and then **Edit rule** to edit it. Enter the required fields as described in the following table.
   - Select an existing rule and then **Delete rule** to delete it.

Table 5-4 Fields

Field	Description
Rule name	Display name of the alert rule. A rule defines the logic that will cause the alert to trigger.An alert policy can have up to five custom rules.
Rule expression SCIM query	Use System for Cross-Domain Identity Management (SCIM) syntax to create the logic that will cause the alert to trigger. You can use **Copy rule from an existing alert policy** to copy the SCIM syntax from a single existing policy. **Tip:** Don't create rules that only apply to specific target databases or times as this will cause errors. See the **Alert condition supported fields** table below for the list of valid fields. See Supported Operators and Tips for Using System for Cross-Domain Identity Management (SCIM) for more information.

Table 5-5 Alert condition supported fields

Field	Description
`Audit type (auditType)`	The type of auditing: `STANDARD`, `FINE_GRAINED`, `XS`, `DATABASE_VAULT`, `LABEL_SECURITY`, `RMAN`, `DATAPUMP`, `DIRECT_PATH_API`
`Client host (clientHostname)`	The host name of the client application that was the source of the event causing the alert.
`Client ID (clientId)`	The client identifier in each Oracle session.
`Client IP (clientIp)`	The IP address of the client application that was the source of the event causing the alert.
`Client program (clientProgram)`	The application from which the audit event was generated. For example SQL Plus or SQL Developer.
`DB user (dbUserName)`	The name of the database user whose actions were audited.
`Error code (errorCode)`	Oracle Error code generated by the action. Zero indicates the action was successful.
`Error message (errorMessage)`	The detailed message on why the error occurred.
`Event (eventName)`	The name of the event executed by the user on the target database. For example `ALTER SEQUENCE`, `CREATE TRIGGER`, or `CREATE INDEX`.
`External user (externalUserId)`	The user ID of the external user of the audit event.

Table 5-5 (Cont.) Alert condition supported fields

Field	Description
Location (auditLocation)	The location of the audit. Currently the value is audit table.
Object(objectName)	Name of the object on the database affected by the action, for example, a table name, file name, or a directory name. Must be in upper case, for example, ALTER_TABLE.
Object owner (objectOwner)	The schema name of the object affected by the action.
Object type (objectType)	Type of object in the source database affected by the action. For example PL/SQL, SYNONYM, or PACKAGE BODY.
Operation (operation)	The name of the action executed by the user on the target database. For example ALTER, CREATE, or DROP.
Operation status (operationStatus)	Status of the event: Success or Failure
OS user (osUserName)	The name of the operating system user for the database session.
Terminal (osTerminal)	The operating system terminal of the user session.
Unified audit policies (auditPolicies)	List of audit policies that caused the current audit event.

Details for an Oracle Data Safe Alert Policy

Oracle Data Safe provides the following information for each Oracle predefined alert policy:

- Policy name
- Severity level of the alert policy; for example, CRITICAL
- Type of alert policy - Currently, all policies are based on auditing.
- Oracle Cloud Identifier (OCID) - You can view and copy this OCID.
- Target databases on which the alert policy is applied
- Rule expression - For example, the expression for the Profile Changes alert policy is `((operation eq_cs "CREATE" OR operation eq_cs "ALTER" OR operation eq_cs "DROP") AND objectType eq_cs "PROFILE")`

View the List of Available Alert Policies

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Alert policies**.

   The list of alert policies is displayed. For each policy, you can view its severity level and description.

View Details for an Alert Policy

1. Under **Security Center**, click **Alerts**.

2. Under **Related Resources**, click **Alert Policies**.
3. Select either the **Oracle predefined alert policies** or **Custom alert policies** tab.
4. Click the name of the alert policy for which you want to view more information.

   The **Alert Policy Details** page is displayed.
5. On the **Alert Policy Information** tab, view the details for the alert policy.
6. For custom alert policies, in addition to the general information and alert policy details, you will see the alert rules associated with the policy.

   In addition to the **Rule name**, **Description**, and **Rule expression**, you will also see:

   - **Rule key**: This is a unique identifier that is automatically generated by Data Safe when a rule is created. It is unique across all rules and policies and can be used in filters in other areas of Data Safe.
   - **Alerts**: This shows the number of alerts that this rule has triggered.

Associate and Apply Alert Policies to Target Databases

You can associate and enable alert policies on target databases from the **Target-Policy Associations** page (recommended) or the **Alert Policy Details** page. On the **Target-Policy** page, you can view all alert policies associated with and enabled on each target database. The **Apply Policy** action associates and enables alert policies in one step.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Target-Policy Associations**. The **Target-Policy Associations** page is displayed.
3. Click **Apply Policy**. The **Apply And Enable Alert Policy To Target Databases** panel is displayed.
4. Select the target databases for which you want to apply the alert policies.

   > **Note:**
   >
   > Currently, you can apply alert policies to a maximum of ten target databases at one time. If you have access to more than ten target databases in your tenancy, you need to choose the **Selected Targets Only** option.

   - To apply an alert policy (or multiple alert policies) to all your target databases (assuming you have ten or less target databases), leave **All Targets** selected. Keep in mind that you require the appropriate permissions in Oracle Data Safe for each target database.
   - To apply an alert policy (or multiple alert policies) to select target databases (up to a maximum of ten target databases), select **Selected Targets Only**. If needed, click **Change Compartment** and select the compartment that contains your target databases. One at a time from the drop-down list, select target databases. To select target databases in a different compartment, click **Add Row**. In the new row, click **Change Compartment** and select a different compartment. One at a time from the drop-down list, select target databases.
5. Select the alert policies.
   - To apply all alert policies, leave **All Policies** selected.

- To apply select alert policies, select **Selected Policies Only**. One at a time from the drop-down list, select alert policies.

6. Click **Apply Policy**.

   The alert policies are applied while the panel is open.

7. Wait until the message **Apply "Profile Changes" on <target database names>** is displayed and has the status **Done**.
8. Click **Close**.
9. Refresh the **Target-Policy Associations** page to view the new associations.

   The target databases have the alert policies enabled by default.

View Target Databases on Which an Alert Policy is Applied

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Alert Policies**.
3. On the right, click the name of the alert policy. The **Alert Policy Details** page is displayed.
4. Next to **Policy Applied On Target Databases**, click **View List** to view the list of target databases on which the alert policy is applied.

   The **Target-Policy Associations** page is displayed. The **Policy Name** filter on the left is automatically set to the alert policy name. If the alert policy isn't applied to any target databases, the message **No Target-Policy Associations Available** is displayed.

View Alert Policies Associated with a Target Database

You can view the alert policies associated with a target database from the **Target-Policy Associations** page. It's useful to apply filters on the page to quickly locate a target database.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Target-Policies Associations**.
3. From the **Compartment** drop-down list on the left, select the compartment that contains the target databases for which you want to view alert policies. Optionally, select **Include child compartments**.
4. From the **Target Databases** drop-down list, select a particular target database.
5. From the **Policy Name** drop-down list, select **All** to view all alert policies associated with your target database. Or, select a particular alert policy name.
6. On the right, view the list of target databases and the alert policies associated with them.

   There is a row for each association. For example, if your target database is associated with two alert policies, there are two rows in the table.

   For each association, you can view whether the alert policy is enabled, the state (Active or Deleted) , when the alert policy was associated with the target database, , and the when the association was last updated
7. To sort the table based on a column, position your cursor over the column header and click the small arrow.

   The table is sorted by the **Time Created** column by default.

Enable or Disable Alert Policies on a Target Database

You can quickly disable an alert policy on a target database from the **Target-Policy Associations** page.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Target-Policy Associations**.

   The **Target-Policy Associations** page is displayed.
3. On the left, set the appropriate compartment, target database, and policy name filters to quickly find the alert policy that you want to enable or disable on your target database.

   The table lists alert policies only for your target database.
4. On the right, select the check box for the rows that pertain to the alert policies that you want to enable or disable.
5. From the **Actions** menu, select **Enable Policy** or **Disable Policy**.

   An **Enable Policy** or **Disable Policy** dialog box prompts you to confirm.
6. Click **Yes**.

Move a Target-Policy Association

You can move a target-policy association resource to a different compartment.

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Target-policies associations**.
3. On the left, filter the list by compartment, target database, and/or policy name.
4. In the table, locate the row that contains the target-policy association that you want to move, and then click the name of your target database.

   The **Target-policy associations details** page is displayed.
5. Click **Move resource**.

   The **Move resource** dialog box is displayed.
6. Select a compartment, and then click **Move resource**.

   The target-policy association is immediately moved to the selected compartment.

Delete a Target-Policy Association

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Target-Policy Associations**.

   The **Target-Policy Associations** page is displayed.
3. On the left, set the appropriate compartment, target database, and policy name filters to quickly find the alert policy that you want to enable or disable on your target database.
4. On the right in the row that pertains to your alert policy and target database, click the target database name.

   The **Target-Policy Associations Details** page is displayed.

5. Click **Delete**.

   The target-policy association is deleted.

View and Manage Alerts

You can view and manage alerts.

Details for an Alert

Oracle Data Safe provides information about each alert on the Alert Information tab. You can navigate to alert details from the Alerts dashboard page.

The following details are provided for each alert:

- Alert name (instance of the alert)
- Target database to which the alert applies
- Alert severity (Critical, High, or Medium)
- Alert status - Whether the alert is open or closed
- Alert type - Currently all alert types are AUDITING
- Policy that generated the alert
- User operation that generated the alert
- Operation status This value can be Succeeded
- When the alert was created and updated
- Oracle Cloud Identifier (OCID) for the alert
- Compartment in which the alert resides
- Operation details - For example, database user

Search For and View an Alert

To quickly find an alert, use the filter options on the Alerts page. You can filter by compartment, time period, and/or target database.

1. Under **Security Center**, click **Alerts**.

   The **Alerts** page is displayed.
2. From the **Compartment** drop-down list, select a compartment that contains the target databases for which you want to find alerts.
3. (Optional) Select **Include Child Compartments**.
4. From the **Time Period** drop-down list, select **Last 24 Hours**, **Last 1 Week**, **Last 1 Month**, **Last 3 Months**, **Last 6 Months**, or **Date Range**.
5. If you selected **Date Range** in step 4, specify the **Time From Month** and **Time To Month** values.
6. From the **Target Databases** drop-down list, select **All** or select a specific target database.
7. If you know the alert's severity, on the **Alerts Summary** tab, click the alert severity level (**Critical**, **High**, **Medium**, or **All Alerts**).

The list of alerts is displayed.

8. If you know the target database for the alert, click the **Targets Summary** tab, and then click a target database name.

   The list of alerts is displayed.

9. Scroll down to the table of alerts and locate the alert for which you want to view details.
10. On the same line as the alert, view the alert status, alert severity, the target database to which the alert belongs, and when the alert was created.
11. Click the alert name to view more detail.

    A page is displayed with alert information and operation (audit) details.

Open or Close an Alert

You can change the status of an alert to open or closed. Setting the status helps to keep your alerts organized.

1. Under **Security Center**, click **Alerts**.

   The **Alerts** page is displayed.

2. Filter the alerts as needed.
3. On the **Alerts Summary** tab, click an alert severity link (**Critical**, **High**, **Medium**, or **All Alerts**). Or, click the **Targets Summary** tab, and then click a target database name.
4. In the list of alert filters, locate the **Alert Status** filter. For **Value**, select **OPEN** or **CLOSED**, or remove the filter.
5. Scroll down to the alert list.
6. To close or re-open one or more alerts on a page, do the following:
   a. Select the check boxes for the alerts on the page.
   b. From the **Actions** menu, select **Close** or **Open**.
   c. In the dialog box, click **Yes** to verify that you want to close or re-open the selected alerts.
7. To close or re-open all alerts displayed on a page, do the following:
   a. Select the check box in the first column header.
   b. From the **Actions** menu, select **Close** or **Open**.
   c. In the dialog box, select **only alerts on the current page** and click **Yes** to verify that you want to close or re-open the selected alerts.
8. To close or re-open all filtered alerts, do the following:
   a. Select the check in the first column header.
   b. From the **Actions** menu, select **Close** or **Open**.
   c. In the dialog box, select **all currently filtered alerts** and click **Yes** to verify that you want to close or re-open all alerts.

> **Note:**
>
> There is a limit of closing or opening 1000 alerts at a time. If you have selected more than 1000 alerts, in the dialog box select to act on **the first 1000 of the currently filtered alerts**. You will have to repeat this step if you wish to close or open more alerts.

9. To first view details for an alert, and then close or re-open it, do the following:
   a. Click the alert's name.
   b. On the alert details page, click **Close** or **Re-Open**.

Move an Alert

You can move an alert to a different compartment.

1. Under **Security Center**, click **Alerts**.

   The **Alerts** page is displayed.
2. Filter the alerts as needed.
3. On the **Alerts Summary** tab, click an alert severity link (**Critical**, **High**, **Medium**, or **All Alerts**). Or, click the **Targets Summary** tab, and then click a target database name.
4. Scroll down and click the name of the alert that you want to move.

   The **Alert Details** page is displayed.
5. Click **Move Resource**.

   The **Move Resource to a Different Compartment** dialog box is displayed.
6. Select a different compartment, and then click **Move Resource**.

   The alert is moved immediately to the new compartment.

Analyze Alerts on the Alerts Dashboard

You can view and analyze auditing-based alerts from the Alerts dashboard.

About the Alerts Dashboard

By default, the Alerts dashboard shows you a summary of alert activity for the last seven days, for all target databases, in the form of charts and tables. You can filter the alerts as needed. The charts and tables are updated based on the filters that you set.

- The **Alerts summary chart** helps you to see the severity of the alerts quickly by comparing the percentage of critical, high, and medium risk alerts.
- The **Open Alerts chart** helps you to see the trend of open alerts by showing you the number of open alerts for the last seven days.
- The **Top 10 alert policies by volume chart** helps you see the trends in the volume of alerts generated by the top 10 alert policies, helping you identify variations over time.
- The **Alerts summary tab** shows you a table consisting of the number of target databases and alerts at each alert severity level (Critical, High, and Medium). It also shows totals for all alerts.

- The **Targets Summary tab** shows you a table consisting of alert totals for each target database. You can view the number of open alerts and the number of critical, high, and medium risk alerts.
- The **Alert policy summary tab** shows you a list of your alert policies, their corresponding severities, number of target databases, and number of alerts.
- The **Notifications tab** shows you what alert notifications and subscriptions you have created. This table will only show Alerts that you have created directly within Data Safe. In addition to displaying existing alert notifications, you can also create new notifications by using the Create notification button. See Create and Modify Event and Alarm Notifications in Alerts for more information.

View and Filter the Alerts Dashboard

You may want to filter the data summarized on the Alerts dashboard. You can filter by compartment, time period, and/or target databases.

1. Under **Security Center**, click **Alerts**.

   The Alerts dashboard is displayed.
2. From the **Compartment** drop-down list, select the compartment that contains the target databases for which you want to view alert summaries. Optionally, you can select **Include child compartments**.
3. From the **Time Period** drop-down list, select the time period for the alert activity.

   You can select **Last 24 Hours**, **Last 1 Week**, **Last 1 Month**, **Last 3 Months**, **Last 6 Months**, or **Date Range**. If you select **Date Range**, specify the beginning (**Time From Month**) and end (**Time To Month**) months.
4. From the **Target Databases** drop-down list, select a specific target database or **All**.

   Only target databases that are contained in the compartment (and child compartments if you selected the option) are listed. If you select **All**, then data for all target databases in the selected compartment is included in the dashboard.

   As you enter the name of a target database, the list of target databases gets filtered.
5. View the **Alerts summary chart** and **Open Alerts chart**.
6. View the **Alerts Summary** and **Targets Summary** tabs.

Analyze Alert Data

1. Under **Security Center**, click **Alerts**.

   The **Alerts** dashboard is displayed.
2. Filter the alerts as needed.
3. To view all the alerts based on a severity level, on the **Alerts summary** tab, click an alert severity link (**Critical**, **High**, **Medium**, or **All Alerts**).

   The relevant alerts are displayed.
4. To view all the alerts based on a target database, click the **Targets Summary** tab, and then click a target database name.
5. At the top of the page, view the filters that are currently applied to the list of alerts.

   These filters are the same as those that were applied to the dashboard.

You can modify, remove, and add filters as needed.

Filter types include **Created on**, **Updated**, **Alert Type**, **Alert Status**, **Alert Severity**, **Operation**, **Operation Time**, **Operation Status**, and **Target Name**.

6. View the summary totals based on the filters set.

   There are totals for the total number of targets, the number of open, critical, high, medium, and low risk alerts; the total number of alerts, and the number of closed alerts.

7. To view the target database names, click **Targets**.

   A **Targets** dialog box is displayed listing the target database names. Click **Close** to close the dialog box.

8. To filter the data in the table below the summary totals, click on any of the other summary totals. For example, to view only critical alerts in the table, click the **Critical** total.

   The table is automatically filtered.

9. In the table at the bottom of the page, view the list of alerts.

10. To add and remove columns from the alert list, from the **Actions** menu, select **Manage Columns**. The **Manage Columns** screen is displayed. Select/deselect columns, and then click **Save Changes**.The following columns are available:

    - **Alert Name** (displayed by default)
    - **Alert Status** (displayed by default)
    - **Alert Severity** (displayed by default)
    - **Target Databases** (displayed by default)
    - **Created On** (displayed by default)
    - **Alert Policy**
    - **Operation**
    - **Operation Status**
    - **Operation Time**
    - **Alert Id**

View and Manage Alert Reports

You can view and manage alert reports.

View an Alerts Report

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.
3. In the **Report Name** column on the right, select a report.

   The report is displayed with its saved filters.

Modifying Columns in an Alerts Report

To add or remove columns in the report, do the following:

1. View a predefined or custom alerts report.

2. Click on the **Actions** drop down menu.
3. Click **Manage Columns**.
   The **Manage Columns** window is displayed.
4. Select columns that you want displayed in the report.
5. Deselect columns that you want to hide in the report.
6. Click **Save Changes**.

Basic Filtering in an Alerts Report

To apply basic filters in the report, do the following:

1. View a custom or predefined alerts report.
2. Click **Another Filter**.
3. Select a filter type, operator, and enter a value. All columns that are available in the report are available as filter types.
4. Click **Apply**.
5. Repeat steps two through four to apply additional filters.

To remove a filter, click the **X** beside the filter row.

To filter the report based on a total category (for example, Login Successes), click the total. The list of audit events in the table at the bottom of the report is automatically updated. To remove the filter, click the total again.

> **Note:**
>
> Only some totals in your report are single-click filters

Advanced Filtering in an Alerts Report

Advanced filtering of alert data can provide flexibility in the way that data is analyzed and reviewed, by allowing organizations to specify complex conditions and multiple criteria that must be met in order for data to be included or excluded from the analysis.

To apply advanced filters in the report, do the following:

1. View a predefined or custom alerts report.
2. Click **Show Advanced SCIM Query Builder**.
3. Use the provided filter builder and dropdowns to type in your filter(s). Advanced filtering uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:
   - `co`: matches resources with an attribute that contains a given string
   - `eq`: matches resources with an attribute that is equal to a given value (not case sensitive)
   - `eq_cs`: matches resources with an attribute that is equal to a given value (case sensitive)
   - `ew`: matches resources with an attribute that ends with a given string

- `ge`: matches resources with an attribute that is greater than or equal to a given value
- `gt`: matches resources with an attribute that is greater than a given value
- `in`: matches resources with an attribute that is equal to any of given values in list
- `le`: matches resources with an attribute that is less than or equal to a given value
- `lt`: matches resources with an attribute that is less than a given value
- `ne`: matches resources with an attribute that is not equal to a given value
- `not_in` : matches resources with an attribute that is not equal to any of given values in list
- `pr`: matches resources with an attribute if it has a given value
- `sw`: matches resources with an attribute that starts with a given string

Operators can be grouped using parentheses to specify the order.

Filters can also be combined using logical operators such as `and` and `or`.

> **Note:**
>
> If you have any basic filters currently applied they will appear in the query builder as well.

4. Click **Apply**.

To clear the query builder, click **Clear**. This will clear any basic filters applied as well.

Example 5-1 Critical or high severity alert advanced filter

```
((severity  eq "CRITICAL" or severity eq "HIGH") and status eq "OPEN")
```

Example 5-2 Critical alerts not on a virtual machine advanced filter

```
(featureDetails.clientHostname ne "vm") and (severity eq "Critical")
```

Example 5-3 Critical alerts on two target databases advanced filter

```
((targetNames eq "ATP01" or targetNames eq "ATP02") and (severity eq
"Critical"))
```

Tips for Using the Filter Builder to Create Advanced Filters

- Pressing the escape key while in advanced filtering mode will clear the whole query.
- Pressing the space key will display the drop down with the list of available attributes or operators.
- Pressing the space key after entering a value like `targetname (demo_tgt)` will enclose the string with quotes: `("demo_tgt")`.
- Pressing enter will close the drop down listing the operators and attribute names.

- If a value like alert name has spaces in it, typing space will enclose the first word within quotes, `"alert name"`. You will have to move the cursor back to the enclosed string and continue typing the rest of the string value.
- If you build a filter in advanced filtering that can't be displayed in basic filters, you can't switch back to basic filtering mode. For example, advanced filters with the or condition can't be displayed in basic filtering.
- A custom report with basic filter can be updated with advanced filter and saved.

For more information about SCIM, see the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644.

For more information about filtering in SCIM, see the filtering section of the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644#section-3.4.2.2.

Create or Change a Schedule for Alert Reports

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.

   The **Reports** page is displayed, showing you a list of alert reports
3. Click the name of the report you would like to view.
4. Click on the **Manage Report Schedule** button.

   The **Manage Report Schedule** panel appears. It will be pre-loaded with either the existing schedule or the default schedule.
5. Change the **Schedule Report Name** if desired.
6. Change the **Compartment** the report is stored in if desired.
7. For **Report Format** select either a PDF or XLS output.
8. Select the **Schedule Frequency**.
   a. If you selected weekly for the schedule frequency, select the day of the week the schedule will run in the **Every** field.
   b. If you selected monthly for the schedule frequency, select the day of the month the schedule will run in the **Day** field.
9. In **Time (in UTC)** select a time.
10. In **Events Time Span** select the time span for which events will be included in the report. For example, selecting Last Months and entering 14 will always pull events from the last 14 months from the time the report is run.
11. Select a **Row Limit**. If unspecified, the default row limit is 200 rows.
12. Click **Save Schedule**.

Generate and Download a PDF or XLS Version of an Alerts Report

You can generate and download a PDF or XLS version of your alerts report. The downloaded report includes the details that you are currently viewing on screen.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.
3. Select the check box for an alert report.

4. Click **Generate Report**.

   The **Generate Report** dialog box is displayed.
5. Select a report format (**PDF** or **XLS**).
6. Enter a display name.
7. (Optional) Enter a description.
8. Select a compartment in which to store your report.
9. (Optional) Set a filter on the number of rows, the target databases, the report start time, and report end time.
10. Click **Generate Report**.
11. Wait until the report is generated.

    A message is displayed stating that the report generation is complete.
12. Download the report. You have two options:
    - In the **Generate Report** window next to **To download report please**, click the **click here** link. A dialog box is displayed providing you options to open or save the document.
    - Click **Close** to close the **Generate Report** window, and then click the **Download Report** button. A dialog box is displayed providing you options to open or save the document.
13. Save the report to your local computer or open and view it.

Create a Custom Alerts Report

You can create a custom report from any alerts report, including the predefined **All Alerts** report. The details saved to the custom reports are those that you are currently viewing on screen. You may want to create a custom report if you want to preserve the filters and columns displayed in a report that you are viewing online. You may also want to store your custom reports in specific compartments.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.
3. Click a report name and modify it as needed. If there aren't any custom reports saved, click the **All Alerts** report and make changes to it.
4. Click **Create Custom Report**.

   The **Create Custom Report** dialog box is displayed.
5. Enter a name for your custom report.
6. (Optional) Enter a description for your custom report.
7. Select the compartment to where you want to save your custom report.
8. Click **Create Custom Report**, and wait for a message that tells you the custom report is created.
9. (Optional) To open and view your custom report, click the **click here** link.
10. (Optional) To return to the report displayed on the screen, click **Close**.

    This report is not your saved report.

Update a Custom Alerts Report

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.
3. In the **Report Name** column on the right, click the name of the custom report that you want to update.

   The report is displayed with its saved filters.
4. Modify the report as needed.
5. Open or close alerts as needed.
6. Click **Save Report**.

   The custom report is updated.

Delete a Custom Alerts Report

When you delete a custom alerts report, the report is permanently deleted and cannot be recovered. You cannot delete the predefined **All Alerts** report.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Reports**.
3. In the **Report Name** column on the right, click the name of the custom report that you want to delete.

   The report is displayed with its saved filters.
4. Click **Delete Report**.

   A **Delete Report** dialog box is displayed, asking you to confirm the deletion.
5. Click **Delete Report**.

View Alert Report History

When an alert report is created, either through a schedule or generated on-demand, it will be listed in **Alert Report History**. The history of reports will be kept for three months. During this time you can view a list of the reports that have been created, details about the reports, and download the reports from **Alert Report History**.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Alert Report History**.

   The Alert Report History table is displayed. It contains information regarding:

   - **Report Name** - The name of the alert report.
   - **Lifecycle State** - Either ACTIVE or UPDATING, shows if the report is currently accessible or if it is being updated.
   - **Report Definition** - Specifies the name of the report that provides data for this scheduled or generated report.
   - **Generated Time** - The date and time the report was created.

- **Report Type** - Generated or Scheduled. Where generated reports are on-demand reports produced outside of the scheduling system and scheduled reports are those produced by the scheduling system.
- **File Format** - PDF or XLS
- **Download Report** - Option to download the report.

3. (Optional) Under **Filters**, narrow down the report history page based on the **Report definition**, **Report type**, **File format**, and **Time period**.

Move an Alert Report to a Different Compartment

Any scheduled or generated alert report from the past three months can be moved to a different compartment that you have access to from Alert Report History.

1. Under **Security Center**, click **Alerts**.
2. Under **Related Resources**, click **Alert Report History**.

   The Alert Report History table is displayed.
3. Click on the name of an alert report from the list.
4. Click **Move Resource**.
5. In the move resource dialog box, select the compartment to move the alert report to. You must have the appropriate `DATA_SAFE_REPORT_MOVE` permissions for the selected compartment.
6. Click **Move Resource**.

   The alert report and Archive Data Retrieval will be moved to the selected compartment immediately.

Create and Modify Event and Alarm Notifications in Alerts

You can create and modify event and alarm notifications in Alerts.

Creating Event Notifications for Alerts

In Data Safe you can create event notifications for Alerts related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create event notifications:

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Reports** or **Target-policy associations** based on what event notifications you'd like to set up.
3. Click the **Notifications** tab.
4. Click **Create notification**.

If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

The **Create notification** side panel will appear.

5. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

> **Note:**
>
> The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

6. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   Optionally, click on **+ Another condition** to add an additional condition to the rule.

   a. Select a **Condition**.
   If you selected **Attribute** in the previous step, select an **Attribute name** and **Attribute values**.

      If you selected **Filter tag** in the previous step, select a **Tag namespace**, a **Tag key**, and a **Tag value**.

   See Alert Event Types in the *Administering Oracle Data Safe* guide for more information on events.

7. Select to either **Create new topic** or to **Select existing topic**.
8. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

9. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
10. Select a **Subscription protocol**.
11. Provide the necessary inputs for the selected subscription protocol.
12. Optionally, click **+ Another subscription** to add additional subscriptions.
13. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.

14. Click **Create notification**.

Creating Alarm Notifications for Alerts

In Data Safe you can create alarm notifications for Alert related events. You can use the quickstart template for common alarm or the advanced alarm notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create alarm notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create alarm notifications:

- Quickstart Template
- Advanced Alarm Notification

Quickstart Template

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Target-policy associations**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Click **Quickstart**.
   A Quickstart templates allow you to select from a list of common alarm scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

   See Alert Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Make a Quickstart **Template selection**.
7. Enter in an **Alarm name**.
8. Select an **Alarm severity**.
9. Enter the **Alerts generation succeeded count**.

10. Enter the **Time that utilization is maintained in minutes**.
11. Select to either **Create new topic** or to **Select existing topic**.
12. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

13. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
14. Select a **Subscription protocol**.
15. Provide the necessary inputs for the selected subscription protocol.
16. Optionally, click **+ Another subscription** to add additional subscriptions.
17. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
18. Click **Create notification**.

Advanced Alarm Notification

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Target-policy associations**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Click **Advanced alarm notification**.
6. Enter in an **Alarm name**.
7. Select an **Alarm severity**.
8. Select an **Event type**.

> **Note:**
>
> The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

Optionally, click on **+ Another condition** to add an additional condition to the rule.

a. Select a **Condition**.

If you selected **Attribute** in the previous step, select an **Attribute name** and **Attribute values**.

If you selected **Filter tag** in the previous step, select a **Tag namespace**, a **Tag key**, and a **Tag value**.

See Alert Event Types in the *Administering Oracle Data Safe* guide for more information on events.

9. Select the **Metric** information.
10. Enter the **Trigger rule** information.
11. Select to either **Create new topic** or to **Select existing topic**.
12. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

13. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
14. Select a **Subscription protocol**.
15. Provide the necessary inputs for the selected subscription protocol.
16. Optionally, click **+ Another subscription** to add additional subscriptions.
17. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
18. Click **Create notification**.

Modifying Event Notifications For Alerts

After creating event notifications in Alerts in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Reports** or **Target-policy associations** based on what event notifications you'd like to modify.
3. Click the **Notifications** tab.
4. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Reports** or **Target-policy associations** based on what event or alarm notifications you'd like to modify.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

To modify the alarm definition:

1. Under **Security center**, click **Alerts**.
2. Under **Related resources**, click **Target-policy associations**.
3. Click the **Notifications** tab.
4. Click on an existing alarm from the **Name** column.
   This will bring you to the Alarm Definitions page which is part of Oracle Cloud Infrastructure (OCI) Monitoring. For more information, see the Monitoring section of the OCI Documentation.

6

Data Discovery

This section discusses how to discover sensitive data in target databases by using the Data Discovery feature in Oracle Data Safe.

Data Discovery Overview

Data Discovery helps you find sensitive data in your Oracle databases.

How Data Discovery Searches for Sensitive Data

Protecting sensitive data begins with knowing what sensitive data you have, and where it is located. Data Discovery's primary means of discovering sensitive data in your target databases is by using sensitive types. Data Discovery also searches for dictionary-based referential relationships to find parent-child relationships. You can also choose to have Data Discovery search for non-dictionary referential relationships (application-level relationships).

Data Discovery searches for sensitive columns in your Oracle databases using the Oracle predefined and user-defined sensitive types that you choose. You tell Data Discovery what to look for, and it finds the sensitive columns that meet your criteria.

To help you validate the discovered sensitive columns, you can choose to collect sample data from your target databases during data discovery. Please be careful when using this feature because the sample data is sensitive data. Only authorized people should be able to collect and view the sample data.

Discovery through Sensitive Types

A **sensitive type** defines regular expressions that help search for sensitive columns based on column names, data, and comments. Oracle Data Safe provides over 170 predefined sensitive types that you can use to search for sensitive data. The predefined sensitive types are organized into categories, making it easy to find and use relevant sensitive types. You cannot modify or delete predefined sensitive types. You can, however, create your own sensitive types and sensitive categories. Data Discovery does not discover sensitive columns that are `object` data types.

The top level categories for predefined sensitive types are as follows:

- **Identification Information:** Includes sensitive types for national, personal, and public identifiers. Examples are US Social Security Number (SSN), Canadian Social Insurance Number (SIN) and other national IDs, Visa Number, and Full Name.
- **Biographic Information:** Includes sensitive types for address, family data, extended PII, and restricted processing data. Examples are Full Address, Mother's Maiden Name, Date of Birth, and Religion.
- **IT Information:** Includes sensitive types for user IT data and device data. Examples are User ID, password, and IP Address.

- **Financial Information:** Includes sensitive types for payment card data and bank account data. Examples are Card Number, Card Security PIN, and Bank Account Number.
- **Healthcare Information:** Includes sensitive types for health insurance data, healthcare provider data, and medical data. Examples include Health Insurance Number, Healthcare Provider, and Blood Type.
- **Employment Information:** Includes sensitive types for employee basic data, organization data, and compensation data. Examples are Job Title, Termination Date, Income, and Stock.
- **Academic Information:** Includes sensitive types for student basic data, institution data, and performance data. Examples are Financial Aid, College Name, Grade, and Disciplinary Record.

Discovery through Dictionary-Based Referential Relationships

Data Discovery also searches the Oracle data dictionary to find relationships between primary key columns and foreign key columns. It then flags those related columns as sensitive. For example, suppose that you have two tables. The first is called `CUSTOMERS`, and it stores information like the customer's first name, last name, and start date. The second table is called `LOCATIONS`, and it stores information about all of your sales locations. The `LOCATION_ID` in the `CUSTOMERS` table is configured as a foreign key and references the primary key, which is `LOCATION_ID` in the `LOCATIONS` table. Data Discovery automatically finds this type of referential relationship. In this example, if there is a sensitive type for location, `LOCATION_ID` in both tables would be captured as sensitive.

Discovery through Non-Dictionary Referential Relationships

In Oracle Data Safe, you have the option to also use non-dictionary referential relationships to find sensitive columns. These are relationships between database columns that are defined in applications, but not in the Oracle data dictionary. Data Discovery uses column name patterns and column data patterns from your selected sensitive types to discover potential relationships between columns.

For example, suppose that a parent table is called `CUSTOMER` and a related table is called `PAYMENT_METHOD`. The sensitive column is `CUST_NAME` in the parent table and `CUST_NM` in the related table. If the related table was created without showing a link in the data dictionary to the parent table (that is, no foreign key information was entered into the data dictionary), the relationship between the parent and related table is a "non-dictionary referential relationship."

Sensitive Data Models

Data Discovery saves the discovery results as a **sensitive data model** to a specified compartment in Oracle Cloud Infrastructure. You can find sensitive data models to which you have access on the Sensitive Data Models page in Oracle Data Safe. The results consist of sensitive columns and referential relationships. When changes occur on a target database, you can perform incremental updates to a sensitive data model, add and remove sensitive columns from the sensitive data model, and manage the referential relationships between the sensitive columns. You can download a sensitive data model, modify it offline, and then upload it into the same or other Oracle Data Safe regions. A sensitive data model is associated with one target database at a time, although you can change that target database if needed.

You can create an empty sensitive data model directly, allowing for a tailored approach to tracking and masking sensitive objects. Instead of running data discovery and removing

unwanted columns, you can create a new sensitive data model with no predefined columns and subsequently add only columns of interest.

To help you understand your sensitive data and for record keeping, Data Discovery provides downloadable reports for sensitive data models and incremental discoveries. Both types of reports provide totals of sensitive tables, columns, and values, and as well as details about the sensitive columns. The sensitive columns are categorized based on their sensitive types.

You can optionally store metadata in a sensitive data model, including sample data and estimated row counts. This information gives you a perspective on the quantity of the different types of sensitive data in your target databases.

You can use a sensitive data model to implement other security controls, such as data masking. For example, you can define a masking policy using an sensitive data model and use it to mask the sensitive data on target databases. You can reuse a sensitive data model for multiple masking policies.

Data Discovery Dashboard in Oracle Cloud Infrastructure

The Data Discovery dashboard provides a high-level view of your sensitive data across the target databases in your selected compartment(s). You can explore key features and workflows with the guided tour option by clicking the "Take the tour" button in the Data Discovery dashboard.

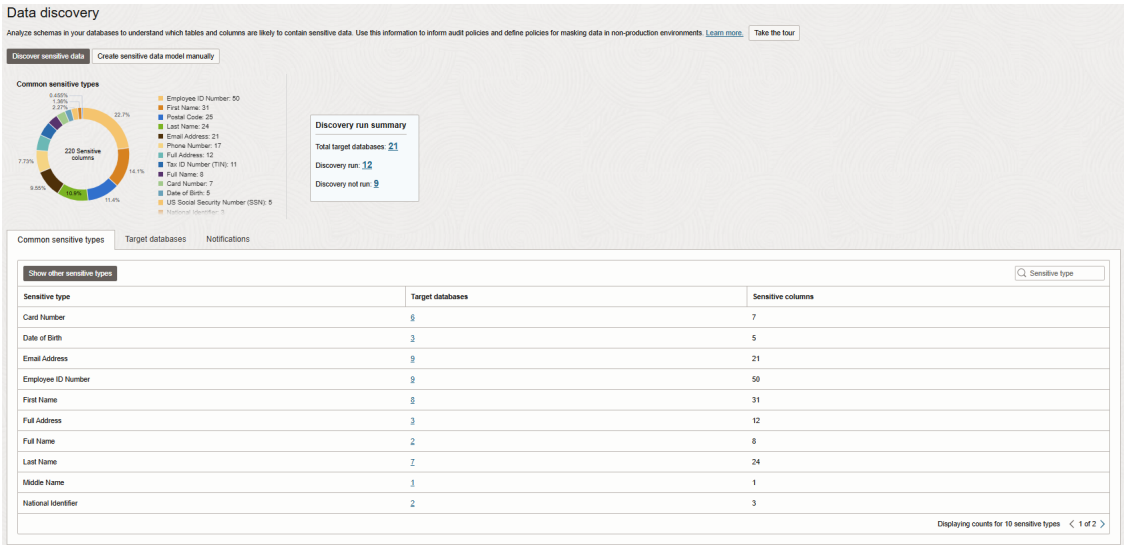
Common sensitive types tab

The **Common sensitive types** tab on the Data Discovery dashboard provides you with an overview of how frequently the 21 common sensitive types are used across your target database fleet. The 21 common sensitive types have been identified by Oracle as the sensitive types that are most likely to be present within a database. Use the **Show other sensitive types** button and the sensitive type search to how frequently other sensitive types are used across your target database fleet.

The **Common sensitive types** chart helps you to identify which sensitive types are most common within your target databases, by showing you a percentage breakdown of the 21 common sensitive types across your target database fleet.

The **Discovery run summary** tables helps you identify if Data Discovery is being well utilized across your target database fleet, by showing you the counts of how many databases have and have not had a sensitive data model created.

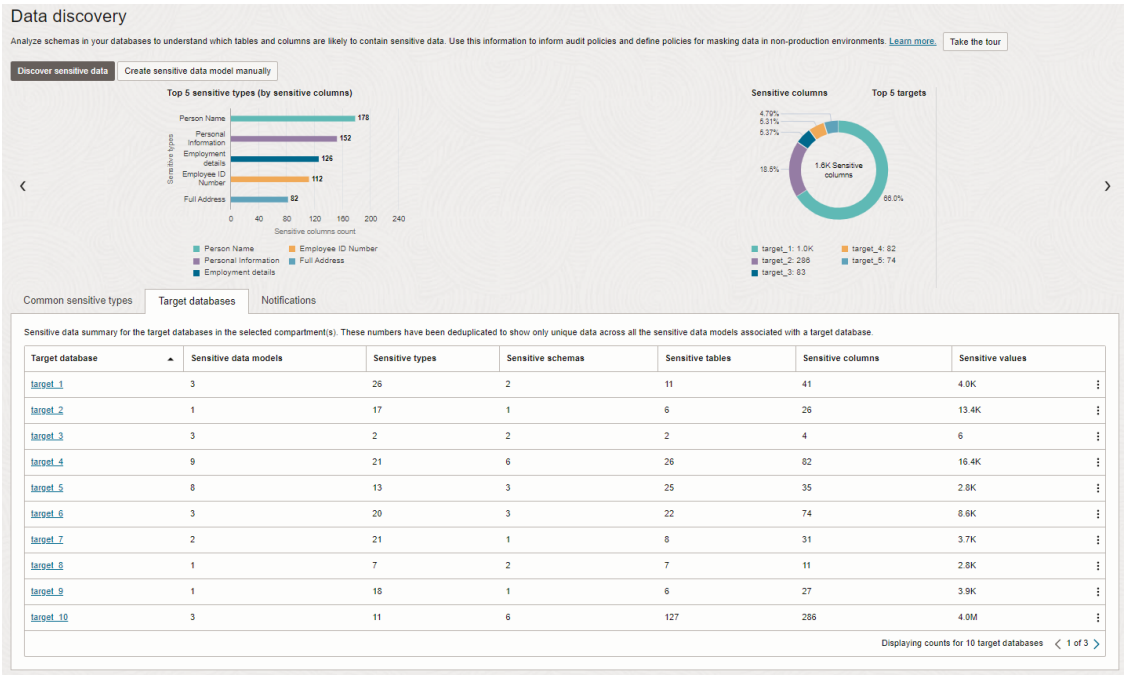
Figure 6-1 Data discovery common sensitive types tab



Target databases tab

The charts at the top of the dashboard focus on your top five target databases. The **Top 5 sensitive types (by sensitive columns)** chart helps you to identify the five sensitive types that are most common within your target databases and how many columns have these sensitive types. The **Sensitive columns** chart helps you to identify which target databases have the most sensitive columns, by showing you a percentage breakdown of sensitive columns across the top five targets. The **Sensitive values** chart helps you to identify which target databases contain the most sensitive values by showing you a percentage breakdown of sensitive values across the five targets.

Figure 6-2 Data discovery target databases tab



The charts are followed by the sensitive data summary for the target databases in the selected compartment(s). The summary lets you compare statistics across the target databases, including the number of sensitive data models created for each target database and the number of sensitive types, sensitive schemas, sensitive tables, sensitive columns, and sensitive values on each target database.

From the sensitive data summary, click on the **Target databases** tab, then click on a target database name to view the **Sensitive Data Models** table, which lists sensitive data models associated with the selected target database. For each sensitive data model, this table shows you the target name, and the quantity of each of the following within the model: sensitive types, sensitive schemas, sensitive tales, sensitive columns, and sensitive values.

You can click on a sensitive data model name to go deeper and view a graph that shows the percentage and distribution of sensitive types within the sensitive data model. This page also provides a **Sensitive Columns** table that lists each sensitive type, its data type, and row count, as well as the schema, table, and column where the type is stored.

Notifications tab

The Notifications tab shows you what event notifications and subscriptions you have created for Data Discovery. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show Events that you have created directly within Data Safe. In addition to displaying existing event notifications, you can also create new notifications by using the Create notification button. See Create and Modify Event Notifications in Data Discovery for more information.

Data Discovery Workflow

Before you create a sensitive data model, you need to do the following:

1. Obtain the appropriate permissions in Oracle Cloud Infrastructure Identity and Access Management, and then register your target database.
2. (Optional) If the schema level statistics are not up-to-date, then gather schema statistics on your target database to ensure accurate results. To do this, run the `dbms_stats.gather_schema_stats` procedure. It is recommended that you run this procedure only when needed, because it is a resource-intensive operation. See GATHER_SCHEMA_STATS Procedures for information about the parameters that you can include. The following example gathers statistics on the `HCM1` schema:

   ```
   exec dbms_stats.gather_schema_stats(ownname => 'HCM1');
   ```

Now you are ready to create a sensitive data model. When working in Data Discovery, follow these general steps when creating a sensitive data model:

1. Provide sensitive data model information and select a target database.
2. (Optional) If the schemas on the target database have been updated since the stated time and date, click **Refresh Database Schemas**.
3. Select the schemas in which you want to find sensitive data. You can also select all schemas. Only non-Oracle mantained schemas are displayed and are selectable.
4. Select the sensitive types to search for on your target database. You can also select all sensitive types.
5. Select optional discovery options, including whether to retrieve sample data and to search for application-level referential relationships.

After your sensitive data model is initially populated with sensitive columns, your next step is to do the following:

1. Review the resulting sensitive columns.
2. Modify the sensitive data model, as needed, so that it accurately reflects the sensitive data in the target database.
   - Perform incremental discoveries.
   - Add and remove columns.
   - Manage referential relationships between sensitive columns.
3. Set up event notifications. For example, you can subscribe to the `Sensitive Data Model Create Begin` event to be automatically informed if a sensitive data model is created.

Over time, you may want to do these tasks:

1. Use the sensitive data model with other target databases. To do this, you can download and upload the sensitive data model into a different Oracle Data Safe region. You can also associate a sensitive data model with a different target database.
2. Move your sensitive data model to a different compartment.
3. Delete your sensitive data model.
4. Create a sensitive data model manually, allowing for a tailored approach to tracking and masking sensitive objects.
   - Instead of running data discovery and removing unwanted columns, you can create a new sensitive data model with no predefined columns and subsequently add only columns of interest.
   - To do this, click the **Create sensitive data model manually** button on the Dashboard or select the **Create sensitive data model manually** check box within the **Discover sensitive data** panel.
   - After the new sensitive data model is created, click **Add columns** to manually add columns of interest to the sensitive data model.

Prerequisites for Using Data Discovery

These are the prerequisites for using Data Discovery:

- **Register the target databases that you want to use with Data Discovery.**
  - If a target database is already registered with Oracle Data Safe by someone else, you need to obtain `READ` permission on the target database resource in Oracle Cloud Infrastructure Identity and Access Management (IAM) to run discovery jobs.
- **Grant the Data Discovery role on the target database.** A Database Administrator can grant this role to the Oracle Data Safe Service Account on the target database.
- **Obtain permission in IAM to use the Data Discovery feature in Oracle Data Safe.** A tenancy administrator can grant these permissions. These resources require permissions:
  - `data-safe-discovery-jobs`
    Requires `manage` permission in order to run discovery jobs.
  - `data-safe-sensitive-data-models`
    Requires `manage` for running discovery jobs and for modifying sensitive data models.
  - `data-safe-sensitive-types`

Requires `manage` for creating sensitive types.

- `data-safe-work-requests`
  Requires `read` permission to view work requests.

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-discovery-family` in the relevant compartments, which would include permissions on all of the resources above. See data-safe-discovery-family Resource in the *Administering Oracle Data Safe* guide for more information.

> **Note:**
>
> Because Data Discovery has moved from the Oracle Data Safe Console to Security Center in Oracle Cloud Infrastructure, an administrator must migrate existing Data Discovery privileges to IAM. After this migration is completed, additional user groups can be granted privileges in IAM to use the Data Discovery feature.

> **See Also:**
>
> The *Administering Oracle Data Safe* guide provides these sections to help with establishing the prerequisites:
>
> - Migrate to Oracle Cloud Infrastructure You can follow the one-time migration procedure described in the guide or you can do the migration manually.
> - Grant Roles to the Oracle Data Safe Service Account on Your Target Database describes the roles required for Data Discovery and for other Oracle Data Safe features.
> - Create IAM Policies for Oracle Data Safe describes the privileges required for each feature in Oracle Data Safe.

Unsupported Data Types, Objects, and Database Features for Data Discovery

These are the unsupported data types for Data Discovery:

- LONG
- RAW
- BFILE
- BLOB
- JSON

These are the unsupported object types for Data Discovery:

- XMLTYPE
- HTTPURITYPE
- XDBURITYPE
- DBURITYPE

- ADT

These are the unsupported database features for Data Discovery:

- External tables
- Temporary tables
- View
- Index
- Nested tables

View Sensitive Types and Categories

In Data Discovery, you can search and view details for sensitive types and sensitive categories.

Search for a Sensitive Type

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Types**.

   By default, all Oracle predefined and user-defined sensitive types are listed. You can apply either filter separately or both at the same time.
3. To search by name, in the **Sensitive Type Name** field under **Filters** on the left, enter a sensitive type name.

   Sensitive types and sensitive categories that match your search criteria are listed.
4. To search by type, from the **Listing Type** drop-down list under **Filters** on the left, select **Oracle Predefined**, **User Defined**, or **All**.
5. To search by only child sensitive types, only parent sensitive categories, or both, from the **Sensitive Category** drop-down list under **Filters** on the left, select **No**, **Yes**, or **All**, respectively.
6. Click **Apply Filters**.

View Sensitive Categories and Sensitive Type Details

On the **Sensitive Types** page in Oracle Data Safe, you can view Oracle predefined sensitive types as well as user-defined sensitive types and categories. It's useful to become familiar with sensitive types and sensitive categories because during data discovery, you choose them to find your sensitive data in your target database.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Types**.

   By default, sensitive categories and all predefined and user-defined sensitive types are listed. Sensitive categories have a `Yes` in the Sensitive Category column. Sensitive types have a`No` value in the same column.
3. To view the details for either a sensitive type or sensitive category, click on its name in the **Name** column.

   For a sensitive type, the following details are displayed:

- Sensitive type name
- Oracle Cloud Identifier for the sensitive type
- Description of the sensitive type
- When the sensitive type was created and last updated
- Parent sensitive category for the sensitive type
- Whether the sensitive type is a sensitive category
- Whether the sensitive type is Oracle predefined
- Column name pattern, column comment pattern, column data pattern, and search type (AND or OR)
- Default masking format

For a sensitive category, the following details are displayed:

- Sensitive category name
- Oracle Cloud Identifier for the sensitive category
- Description of the sensitive category
- When the sensitive category was created and last updated
- Whether the sensitive category is a sensitive category
- Whether the sensitive category is Oracle predefined
- A table containing a list of the child sensitive types that are a part of the parent sensitive category. This table specifies the:
  - Child sensitive type name
  - Child sensitive type description
  - Whether the child sensitive type is also a sensitive category
  - Whether the child sensitive type is Oracle predefined

Note: To view the details for a child sensitive type, click on its name in the **Name** column.

4. To return to the list of sensitive types, click **Sensitive Types** in the breadcrumb at the top of the page.

Create Sensitive Types and Categories

In Oracle Data Safe, you can create your own sensitive types, sensitive categories, and sensitive type groups.

Create a Sensitive Type

When creating a sensitive type, you can provide one or more patterns (regular expressions) that should be used to discover sensitive columns. You can provide a column name pattern, column comment pattern, column data pattern, and a search type (AND/OR). Data Discovery performs case-insensitive pattern matching.

For a user-defined sensitive type, you can assign a default masking format, is used to mask the columns discovered using this sensitive type. When creating a user-defined sensitive type, you must assign it to a compartment.

1. Under **Security Center**, click **Data Discovery**.

2. Under **Related Resources** in Security Center, click **Sensitive Types**.
3. Click **Create Sensitive Type / Category**.

   The **Create Sensitive type / Category** window is displayed.
4. In the **Name** field, enter a name for your sensitive type.
5. From the **Compartment** drop-down list, select the compartment in which you want to store the sensitive type.
6. (Optional) In the **Description** box, enter an explanation of your sensitive type.
7. From the **Parent Sensitive Category** drop-down list, select the sensitive category to which you want your sensitive type to belong.
   - If needed, click **Change Compartment** and select a different compartment.
   - You can choose a user-defined sensitive category as a parent category, but not a category used by predefined sensitive types.
8. Leave the **Sensitive Type** tile selected.
9. (Optional) To use a predefined sensitive type as a starting point, select a predefined sensitive type from the **Create Like** drop-down list. If you want to select a user-defined sensitive type and it is located in a different compartment, click Change Compartment, browse to and select the correct compartment. The compartment doesn't matter if you are selecting an Oracle predefined sensitive type.
10. Configure one or more of the following patterns.
    - **Column Name Pattern**: Enter a regular expression that should be used to match column names.
    - **Column Comment Pattern**: Enter a regular expression that should be used to match column comments.
    - **Column Data Pattern**: Enter a regular expression that should be used to match column data.
11. For **Search Type**, select **Or** or **And**.
    - The **Or** operator means that any of the patterns can match for a candidate sensitive column.
    - The **And** operator means that all of the patterns must match for a candidate sensitive column.
    - If the column doesn't include a comment, the column comment pattern matching is skipped. Similarly, if the column doesn’t contain data, the data pattern matching is also skipped.
12. (Optional) From the **Default Masking Format** drop-down list, select a masking format for Oracle Data Safe to use by default when masking sensitive columns discovered by your sensitive type.
13. (Optional) Click **Show Advanced Options**, and define tags.
14. Click **Create Sensitive Type**.

    The **Sensitive Type Details** page is displayed.

Create a Sensitive Category

1. Under **Security Center**, click **Data Discovery**.

2. Under **Related Resources** in Security Center, click **Sensitive Types**.
3. Click **Create Sensitive Type / Category**.

   The **Create Sensitive type / Category** window is displayed.
4. In the **Name** field, enter a name for your sensitive category.
5. Select a compartment in which to store your sensitive category.
6. (Optional) Enter a brief description of your sensitive category.
7. (Optional) Select a parent sensitive category.
8. Click the **Sensitive Category** tile.

   Notice that button at the bottom changes from **Create Sensitive Type** to **Create Sensitive Category**.
9. (Optional) Click **Show Advanced Options**, and define tags. Click **Create Sensitive Category**.

Create and Manage a Sensitive Type Group

Creating a sensitive type group allows you to select a subset of sensitive types that can be used throughout Data discovery. Oracle has created a **Common sensitive types** group consisting of commonly used sensitive types that is available in all compartments.

Ensure you have the proper permissions to use sensitive type groups, see data-safe-sensitive-type-group Resource in the *Administering Oracle Data Safe* for more information.

Create a Sensitive Type Group

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive types**.
3. Click the **Sensitive type groups** tab.
4. Click **Create sensitive type group**.
5. Name your sensitive type group.
6. Select which compartment the sensitive type group will be stored in.
7. Select the sensitive types that you want included in the sensitive type group.
8. Click **Create sensitive type group**.

Manage a Sensitive Type Group

Sensitive types can be added or removed from a sensitive type group after it is created.

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive types**.
3. Click the **Sensitive type groups** tab.
4. Select the sensitive type group you want to manage from the list.
5. To add sensitive types, click **Add sensitive type**.
6. To remove sensitive types, select the sensitive type(s) to remove and click **Remove sensitive type**.

Tips for Creating Sensitive Types

The following topics help you to write patterns for sensitive types. For more information about regular expressions, see Regular Expressions.

Column Name Pattern

A column name pattern is a regular expression that is used to match column names during data discovery. For example, to search for columns containing Social Security numbers, you could define the following column name pattern:

```
(^|[_-])SSN($|[_-])|(SSN|SOC.*SEC.*).?(ID|NO|NUMBERS?|NUM|NBR|#)
```

The regular expression checks for specific keywords in column names. It matches column names, such as `PATIENT_SSN`, `SSN#`, `SOCIAL_SECURITY_NUMBER`, and `EMPLOYEE_SOC_SEC_NO`.

Tips for creating column name patterns:

- Consider when to use `.?` and `.*`. Use `.?` if you want to allow zero or one character, and use `.*` to allow any number of characters. For example, you could use `SOCIAL.?SECURITY.?NUMBER` or `SOC.*SEC.*NUMBER` depending upon how strict you want the regular expression to be.
- To get an exact match of a word or a match if the word is part of a column name, use `(^|[_-])<WORD>($|[_-])`. The pattern finds an exact match and variations of `<WORD>` plus the characters `_-` before or after the word.
- Whenever searching for columns containing numbers, you could use keywords like `(ID|NO|NUMBERS?|NUM|NBR|#)`.
- To match singular and plural words, if applicable, use `S?`. For example, use `CODES?` to match `CODE` and `CODES`.
- To match dates, use `(DT|DATE)` and the reverse pattern. For example, you could use the following pattern to match `BIRTH_DATE` and `DATE_OF_BIRTH`:

  ```
  BIRTH.?(DT|DATE)|(DT|DATE).*BIRTH
  ```

Column Comment Pattern

A column comment pattern is a regular expression that is used to match column comments during data discovery. Sometimes column names are obscure and therefore, metadata is entered as a comment for a database column. Data Discovery can search these comments and potentially find more sensitive data. For example, to search for columns containing Social Security numbers, you could define the following column comment pattern:

```
\bSSN#?\b|SOCIAL SECURITY (ID|NUM|\bNO\b|NBR)
```

The regular expression checks for specific keywords in column comments. For example, it matches the column comment `Contains social security numbers of employees`.

Tips for creating column comment patterns:

- Avoid using `.*` in column comments to reduce false positives.
- Use `\b<word>\b` to search for a specific word. It avoids matching words that contain `<word>`. For example, the regular expression `\bNO\b` matches `social security no` but not `social security notification`. Similarly, the regular expression `\bSECT\b` does not match the word `SECTOR`, and `\bCULT\b` does not match the word `CULTURE`.
- Whenever searching for columns containing numbers, you can use keywords like `(ID|\bNO\b|NUM|NBR|#)`.

Column Data Pattern

A column data pattern is a regular expression that is used to match the actual column data during data discovery. For example, to search for columns containing Social Security numbers, you could define the following column data pattern:

```
^[0-9]{3}[ -]?[0-9]{2}[ -]?[0-9]{4}$
```

The regular expression checks for 9-digit numbers. A number can be either numeric or can have three parts separated by hyphens or spaces. It matches numbers like `383368610` and `383-36-8610`.

Tips for creating column data patterns:

- Ensure that the data pattern is as specific as possible to avoid false positives.
- See whether it is logical to have a data pattern. If the data pattern is too broad, it can result in false positives. If it does not add any value, you could decide not to add the data pattern for a sensitive type.
- If you want to use a broad data pattern, you could use the `And` search operator to reduce false positives.

Search Pattern

The search pattern indicates how the column name, comment and data patterns of a sensitive type should be used to discover sensitive columns. There are two search options: AND and OR.

The **AND** search option ensures that all the provided patterns of a sensitive type must match for identifying a column as sensitive. For example, if a sensitive type has name, comment, and data patterns, they must match a column's name, comment, and data respectively, for identifying that column as sensitive. The following table covers the various possible combination of the patterns provided for a sensitive type and the corresponding AND search behavior.

Patterns Present in a Sensitive Type	Search Behavior
Name, Comment, and Data	Name AND Comment AND Data
Name and Data	Name AND Data
Name and Comment	Name AND Comment
Comment and Data	Comment AND Data
Name	Name
Comment	Comment
Data	Data

The **OR** search option provides some flexibility to identify a column as sensitive even if only some of the patterns of a sensitive type match. For example, if a sensitive type has name and comment patterns, a column is identified as sensitive even if only the name pattern (or comment pattern) matches the column's name (or comment). If a sensitive type has all three patterns, the data pattern must match along with either the name pattern or the comment pattern (or both). The following table covers the various possible combination of the patterns provided for a sensitive type and the corresponding OR search behavior.

Patterns Present in a Sensitive Type	Search Behavior
Name, Comment, and Data	Data OR (Name AND Data) OR (Comment AND Data)
Name and Data	Data OR (Name AND Data)
Name and Comment	Name OR Comment
Comment and Data	Data OR (Comment AND Data)
Name	Name
Comment	Comment
Data	Data

Manage Sensitive Types

You can manage sensitive types.

Update a User-Defined Sensitive Type

You can modify user-defined sensitive types, but not Oracle predefined sensitive types.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Types**.

   By default, all the predefined and user-defined sensitive types are listed.
3. Search for and click the name of the user-defined sensitive type that you want to update.

   The **Sensitive Type Details** page is displayed.
4. Click **Edit**.

   The **Edit Sensitive Type** window is displayed.
5. Modify the parameters, and then click **Save**.

Move a User-Defined Sensitive Type to a Different Compartment

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Types**.

   By default, all Oracle predefined and user-defined sensitive types are listed.
3. Search for and click the name of the user-defined sensitive type that you want to move.

   The **Sensitive Type Details** page is displayed.
4. Click **Move Resource**.

   The **Move Resource to a Different Compartment** dialog box is displayed.

5. Select a compartment, and then click **Move Resource**.

Delete a User-Defined Sensitive Type

Deleting a user-defined sensitive type is permanent. You cannot delete Oracle predefined sensitive types.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Types**.

   By default, all Oracle predefined and user-defined sensitive types are listed.
3. Search for and click the name of the user-defined sensitive type that you want to delete.

   The **Sensitive Type Details** page is displayed.
4. Click **Delete**.
5. In the dialog box, click **Delete** to confirm.

Export and Upload User-Defined Sensitive Types

Exporting user-defined sensitive types allows you to export existing sensitive types and categories from one region or tenancy and then upload the same sensitive types and categories into other regions or tenancies using XML. This minimizes the time required to define the same sensitive types and categories multiple times across different regions or tenancies.

In order to export and upload sensitive types and categories, you need to obtain permissions on the `data-safe-sensitive-types-export` and `data-safe-sensitive-types` resources. See data-safe-discovery-sensitive-types-export Resource and data-safe-sensitive-types Resource for more information.

Export user-defined sensitive types

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive types**.
3. Click **Export sensitive types as XML**.
4. Enter a name for the export resource.
5. Set the compartment that the export resource will be saved in.
   The export resource will be stored in the selected compartment for three months, and will be automatically deleted after that. During the three months while the resource is available, you can access it to download the XML file containing the exported sensitive type(s). See *Download exported sensitive types from the export resource* for more information.
6. Select which sensitive types and/or categories you want to export.
   You will see all sensitive categories and types available within the root compartment and all child compartments, regardless of what compartment you're currently in.

   When selecting sensitive types and categories that are children of other sensitive categories, the hierarchy will be preserved in the export, i.e, the parent sensitive categories will be exported as well. However, sibling sensitive types and categories will not be exported unless they are explicitly selected for export.

   Ensure that any sensitive categories that you select contain at least one sensitive type. You can't export an empty sensitive category.

7. Click **Export sensitive types**.
   You will be brought to the export resource details.
8. Click **Download as XML**.

Download exported sensitive types from the export resource

If it's been less than three months since you initiated the export of sensitive types, then you can access the XML of that export from the **Sensitive type exports** resource.

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive type exports**.
3. Click on the desired export from the list.
   You will be brought to the export resource details.
4. Click **Download as XML**.

Upload user-defined sensitive types

This action is typically done in a different region or tenancy from where the export took place.

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive types**.
3. Click **Upload sensitive types as XML**.
4. Select the compartment that the sensitive types will be uploaded into.
5. Select the XML file of exported sensitive types from your local system to upload.
6. Click **Upload sensitive types**.
   When uploading sensitive types and categories that were originally the children of other sensitive categories, the hierarchy is preserved in the upload, i.e, the parent sensitive categories will be created in the destination region or tenancy as well.

Related Topics

- Create Sensitive Types and Categories
  In Oracle Data Safe, you can create your own sensitive types, sensitive categories, and sensitive type groups.

Create Sensitive Data Models

You can create sensitive data models by discovering sensitive data in Data Discovery or by creating an empty sensitive data model and manually adding columns of interest.

Create a Sensitive Data Model Through Data Discovery

1. Under **Security center**, click **Data discovery**.
2. Click **Discover sensitive data**.
3. For **Sensitive data model information**, do the following:
   a. Enter a name for the sensitive data model or leave the default name as is.
   b. Select a compartment in which to store your sensitive data model.
   c. Optionally, enter a description for your sensitive data model.
   d. Select a target database.

e. If you need to switch compartments, click **Change compartment**, and browse to and select a different compartment.

f. Click **Next**.

4. For **Select schemas**, select the schemas that you want Data Discovery to search, and then click **Next**. Only non-Oracle maintained schemas are displayed and are selectable.

   - (Optional) If the schemas on the target database have been updated since the stated time and date, click **Refresh database schemas**.
   - To select all the schemas at once, select the check box to the left of the **Schema name** column title.
   - To search for a schema, enter part of all of your schema's name in the search box in the upper-right corner, and then click **Search**. The name is case-sensitive.
   - At the bottom right, click the left and right arrow buttons to navigate the pages.

5. Optionally, for **Select tables for schema**, select tables for selected schemas from the target database. If selected, discovery will be run only on selected tables of the schema. Alternatively, you can skip this step and proceed to the next if you want all tables for the selected schemas to be scanned.

6. For **Select sensitive types**, select the categories of sensitive types and/or the individual sensitive types that you want to use to discover sensitive data, and then click **Next**.

   Use the **Select from sensitive type group** section to discover from the sensitive types in any of your sensitive type groups or from the 21 most popular sensitive types in the **Common sensitive types** group created by Oracle. By limiting the selection of sensitive types that are likely to be present within your target database, you decrease the time that it will take to create a sensitive date model. You may select additional sensitive types in the **All sensitive types** section.

   Use the **All sensitive types** section

   - To view all categories and sensitive types, toggle the **Expand All** slider to the right.
   - To view sensitive types within a sensitive category, expand individual check boxes.
   - To view only Oracle Predefined sensitive types and categories, toggle **Show only Oracle Predefined Sensitive Types**

7. For **Select Discovery Options**, do the following:

   a. (Optional) To collect sample data values from the target database, select **Collect, display and store sample data**. The collected data is automatically deleted when you delete the sensitive data model.

   b. (Optional) Select **Discover application level (non-dictionary) referential relationships**. This option uses column name and data patterns from the selected sensitive types. The discovered relationships can span across schemas, including those not selected on the **Select Schemas** page.

   > **Note:**
   >
   > See Discovery through Non-Dictionary Referential Relationships for more information.

8. Click **Create Sensitive Data Model**.

The **Sensitive Data Model Details** page is displayed. When the data discovery job is completed successfully, a status of **ACTIVE** is displayed and details about the sensitive data model are displayed.

9. On the **Sensitive Data Model Information** tab, review the chart to identify which sensitive types and sensitive categories have the most sensitive data.
10. Scroll down to the **Sensitive Columns** section, and review the sensitive columns. You can organize the data three ways by selecting one of the following options from the drop-down list:
    - **Flat View (default):** Lists sensitive columns, sorted alphabetically by either schema, table, or column.
    - **Sensitive Type View:** Organizes the results by sensitive type.
    - **Schema View:** Organizes the results by schema.
11. To filter the list of sensitive columns, do the following:
    a. Click **+ Add Filter**.
    b. In the first drop-down list, select **Column Name**, **Schema Name**, **Table Name**, **Sensitive Type**, or **Relation with Parent**.
    c. In the second drop-down list, select an operator.
    d. In the box, enter a value. Note that this field is case-sensitive. Enter an exact match.
    e. To add another filter, click **+ Add Filter** and repeat the steps b through d.
    f. When all your filters are created, click **Apply**.
    g. To remove a filter, click the **X** button next to the filter.
12. Examine the referential relationships.

Create a Sensitive Data Model Manually

1. Under **Security center**, click **Data discovery**.
2. Click **Create sensitive data model manually**.
3. For **Sensitive data model information**, do the following:
    a. Enter a name for the sensitive data model or leave the default name as is.
    b. Select a compartment in which to store your sensitive data model.
    c. Optionally, enter a description for your sensitive data model.
    d. Select a target database.
    e. If you need to switch compartments, click **Change Compartment**, and browse to and select a different compartment.
4. Click **Create sensitive data model manually**.

   The **Sensitive Data Model Details** page is displayed. When the data discovery job is completed successfully, a status of **ACTIVE** is displayed and details about the sensitive data model are displayed.
5. To manually add columns to the sensitive data model, do the following:
    a. Scroll down to the **Sensitive Columns** list and click **Add Columns**.

       The **Add Columns** window is displayed.

b. (Optional) If the schemas on the target database have been updated since the stated time and date, click **Refresh Database Schemas**.

c. Find sensitive columns by entering or selecting one or more of the following items, and then click **Search**:

Schema name

Table name

Column name

A list of sensitive columns that match your selection criteria are displayed.

d. Add the sensitive type for each column by selecting a sensitive type from the drop-down list.

e. Select the columns that you want to add to your sensitive data model, and then click **Add Columns**.

To select all the columns, select the **All columns** radio button. To select all columns on the current page, select the check box next to the Schema column heading.

View Sensitive Data Models

In Data Discovery, you can search and view details for sensitive data models.

Search for a Sensitive Data Model

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.

   A list of sensitive data models to which you have access is displayed. In the table, you can view the states (for example, CREATING, ACTIVE, and so on), descriptions, when the sensitive data models were created, and when they were last updated.
3. Under **List Scope**, select the compartment that contains your sensitive data model. Optionally select **Include child compartments** to include sensitive data models in the list from child compartments.
4. To filter the list of sensitive data models, under **Filters**, do the following:

   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).

   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.

   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.

   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.

   e. Click **Apply Filters**.

View Details for a Sensitive Data Model

Sensitive data models are listed on the **Sensitive data models** page. You can view details for the sensitive data models to which you have access.

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
3. Search for and click the name of a sensitive data model to view its sensitive columns and details.
4. On the **Sensitive data model information** tab, review the **Top 5 sensitive types (by sensitive columns)** chart to identify which sensitive types and sensitive categories have the most sensitive data. Click on a sensitive type within the chart to automatically filter the sensitive data model and focus on that specific type.
5. To view the list of sensitive columns, scroll down to the **Sensitive columns** section. You can organize the data three ways by selecting one of the following options from the drop-down list:
   - **Flat view (default)**: Lists sensitive columns by either the schema, the table, or the column name in alphabetical order.
   - **Sensitive type view**: Organizes the results by sensitive type.
   - **Schema view**: Organizes the results by schema.
6. To explore the list of sensitive columns, do the following:
   a. Select one or more schemas from the **Schema name** list. Click **Load more** if there are more than 1000 schemas and your desired schema is not already listed.
   b. Select one or more tables from the **Table name** list. Click **Load more** if there are more than 1000 tables and your desired table is not already listed.
   c. Select one or more columns from the **Column name** list. A list of columns will only be available once either a schema or table is selected. Click **Load more** if there are more than 1000 columns and your desired column is not already listed.
   d. Click **Show more options** to filter by sensitive type or relationship with parent as well.
   e. Select one or more sensitive types from the **Sensitive type** list. Click **Load more** if there are more than 1000 sensitive types and your sensitive type is not already listed.
   f. Select one of the relationships with parent from the **Relation with Parent** list.
   g. When all of your filters are created, click **Apply**.
   h. To remove a filter, click the **X** button next to the selected item.
7. To view the selected schemas related to the sensitive data model, you can do the following:
   - To view the selected schemas discovery was performed on, on the **Sensitive data model information** tab, click the **View details** link next to **Selected schemas for discovery**. The **Schemas for discovery** page is displayed. Here you can view the schemas included in the discovery for the selected sensitive data model.
8. To view the selected sensitive types related to the sensitive data model, you can do the following:
   - To view the selected sensitive types discovery was performed on, on the **Sensitive data model information** tab, click the **View details** link next to **Selected sensitive types for discovery**. The **Sensitive types for discovery** page is displayed. Here you can view the sensitive types included in the discovery for the selected sensitive data model.
9. To view the sensitive schemas discovered, you can do the following:
   - To view the sensitive schemas that were discovered, on the **Sensitive data model information** tab, click the **View details** link next to **Sensitive schemas discovered**.

The **Sensitive schemas** page is displayed. Here you can view the sensitive schemas that were discovered for the selected sensitive data model.

Note: Even if discovery is performed on only a subset of tables within a schema, that schema will still be listed in the **Sensitive schemas** page.

10. To view the sensitive types discovered, you can do the following:

    - To view the sensitive types that were discovered, on the **Sensitive data model information** tab, click the **View details** link next to **Sensitive types discovered**. The **Sensitive types discovered** page is displayed. Here you can view the sensitive types that were discovered for the selected sensitive data model.

      Note: The sensitive types displayed are those that resulted from the latest discovery run and do not change if sensitive types are dropped or altered in the current version of the sensitive data model.

11. To view what actions have been taken on your sensitive objects, click **View activity** in the **Audit records** column.

    > **Note:**
    >
    > You need to have audit policies enabled that monitor the sensitive objects to see the database activities.

    An activity auditing report with predefined filters based on the sensitive data selected is displayed.

12. To view the work requests related to the sensitive data model, you can do the following:

    a. To view the latest work request, on the **Sensitive data model information** tab, click the **View details** link next to **Work Request**. The **Work Request** page is displayed. Here you can view the work request information, log messages, and error messages (select **Error Messages** under **Resources**).

    b. To view all the work requests for the past seven days (work requests are stored for only 7 days in Oracle Cloud Infrastructure), under **Resources**, click **Work Requests**. From here, you can view the status (for example, SUCCEEDED or FAILED), percent completed, date started, and date finished details for each work request. Click a particular work request to view its log messages and error messages.

    c. (Optional) If there was a work request failure, notice the error message displayed at the top of the page, for example, "There is at least one work request associated with this policy that has failed."

13. To view referential relationships, under **Resources**, click on **Referential relationships**.

14. To create a masking policy based on the sensitive data model, click the **Create masking policy** button at the top of the **Sensitive data model details** page.

    - The **Create masking policy** page will open. Follow the steps outlined in **Create a Masking Policy Starting From a Sensitive Data Model**.

Update Sensitive Data Models

There are many reasons why you may need to update a sensitive data model after you discover sensitive columns on your target database. Perhaps changes on the database have occurred or you may need to fine-tune the discovery results. With Data Discovery, you can perform incremental discoveries and make manual changes to your sensitive data model.

You can also manually edit the XML version of a sensitive data model in a text editor. To obtain an XML format of your sensitive data model, you need to generate it first and then download it from the sensitive data model's page. See Download or Upload a Sensitive Data Model in XML Format.

Perform an Incremental Discovery of Sensitive Data on Your Target Database

If columns are added, deleted, or modified on your target database after you run a data discovery job, you can perform an incremental discovery to update your sensitive data model. This operation compares the sensitive columns in your sensitive data model to those on the target database and informs you of the differences. If needed, you can adjust the schemas and sensitive types that Data Discovery uses during the incremental discovery on the target database.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Click the name of the sensitive data model for which you want to perform an incremental discovery of sensitive data.
4. Under **Resources**, click **Latest Incremental Discovery**.

   The **Incremental Discovery** section is displayed.
5. Click **Run Discovery Now**.

   The **Run Discovery Now** dialog box is displayed.
6. To run the incremental discovery with the same scope as the initial discovery job, select **Run the incremental discovery with the same scope as the initial sensitive data discovery of this sensitive data model**, and click **Submit**.

   Note the previously selected tables will be honored for the scope (either all tables or the subset that were selected).

   Be aware before proceeding that the results from the previous incremental discovery are not shown after you start this operation.

   The incremental discovery job is started and the job status is set to **CREATING**.
7. To change the scope before running the incremental discovery job, select **Adjust the scope for the incremental discovery**, click **Submit**, and then configure the **Options for Incremental Discovery** page:

   a. For **Provide basic information**: Enter a name for the discovery job, select a compartment to store the discovery job, and then click **Next**.

   b. For **Select schemas**: Select the schemas that you want the incremental discovery to search, and then click **Next**.

      - To select all schemas, select **All schemas** or select the check box to the left of the **Schema name** column title.
      - To search for a schema, enter part or all of your schema's name in the search box in the upper-right corner, and then click **Search**. The name is case-sensitive.
      - To navigate the pages, click the left and right arrow buttons at the bottom of the page.

   c. Optionally, for **Select tables for schema**, select tables for selected schemas from the target database. If selected, discovery will be run only on selected tables of the

schema. Alternatively, you can skip this step and proceed to the next if you want all tables for the selected schemas to be scanned.

d. For **Select sensitive types**, select the categories of sensitive types and/or the individual sensitive types that you want to use to discover sensitive data, and then click **Next**.

   Use the **Select from sensitive type group** section to discover from the sensitive types in any of your sensitive type groups or from the 21 most popular sensitive types in the **Common sensitive types** group created by Oracle. By limiting the selection of sensitive types that are likely to be present within your target database, you decrease the time that it will take to create a sensitive date model. You may select additional sensitive types in the **All sensitive types** section.

   Use the **All sensitive types** section

   - To view all categories and sensitive types, toggle the **Expand All** slider to the right.
   - To view sensitive types within a sensitive category, expand individual check boxes.
   - To view only Oracle Predefined sensitive types and categories, toggle **Show only Oracle Predefined Sensitive Types**

e. For **Select discovery options**: Optionally select the following options:

   - **Collect, display, and store sample data**
   - **Discover application-level (non-dictionary) referential relationships**

f. Click **Run Discovery Now**.

   Be aware before proceeding that the results from the previous incremental discovery are not shown after you start this operation.

The incremental discovery job is started and the status of the job is set to **CREATING**.

8. (Optional) To view the work request details, click the **View Details** link.

   The **Work Request** page shows you the progress of the incremental discovery job. You can suspend or abort the job at this time.

9. After the discovery job is successfully completed, review the information in the **Incremental Discovery** section to learn about the changes on your target database:

   - Status of the discovery job
   - Last incremental discovery date
   - Selected schemas for incremental discovery
   - Selected sensitive types for incremental discovery
   - Work request
   - Total number of new columns
   - Total number of deleted columns
   - Total number of modified columns
   - Details about each discovered column, including schema, table, column, column status in target database (for example, NEW or DELETED), sensitive type, parent column, data type, planned action, sample data, and estimated row count

10. For each column listed in the incremental discovery table, select its check box and click **Approve** or **Reject**.

    - If you click **Approve**, the **Approve Discovery Results** dialog box is displayed asking if you want to approve the selected column. Click **Approve** if you are sure; otherwise,

click **Cancel**. Approving the selected columns marks the discovery results to add new columns, remove deleted columns, or update modified columns. This action does not update the sensitive data model automatically. The **Planned Action** column shows **Approved** after you click **Approve**. You can always change to **Reject**, if needed.

- If you click **Reject**, the **Reject Discovery Results** dialog box is displayed asking if you are sure you want to reject the selected discovery results. Click **Reject** if you are sure; otherwise, click **Cancel**.

11. After you have approved and/or rejected each discovered incremental changes, click **Apply to SDM**.

    The **Apply To Sensitive Data Model** dialog box is displayed asking if you want to apply the results to the sensitive data model.

12. Click **Submit**.

    This operation updates the sensitive data model with all the sensitive columns you approved. A message states **Sensitive Data Model Updated Successfully**. If you run another incremental discovery job, your results will be overwritten.

View the History of Incremental Discovery

Data Discovery maintains a history of each incremental discovery job on a sensitive data model (SDM). For each job, you can view when the incremental discovery was performed, the selected schemas for the incremental discovery, the selected sensitive types, what column changes were approved or rejected, and whether the changes were applied to the SDM.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.

   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model for which you want to view the history of incremental discovery.
4. Under **Resources**, click **History of Incremental Discoveries**.

   Sensitive data model details are displayed and past incremental discovery jobs are listed.
5. Select the incremental discovery job that you want to view.

   The **Discovery Job Results** page shows you the details for the incremental discovery in a read-only table. You can view information about each discovered column, including schema, table, column, column status in target database (for example, NEW or DELETED), sensitive type, parent column, data type, estimated row count, planned action, and whether the change was applied to the SDM.
6. To return to the history of incremental discoveries, click **Close**.

Add New Sensitive Columns to a Sensitive Data Model

You can add new sensitive columns to an existing sensitive data model on the sensitive data model's page.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.

   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model to which you want to add sensitive columns.

4. Scroll down to the **Sensitive Columns** list and click **Add Columns**.

   The **Add Columns** window is displayed.

5. (Optional) If the schemas on the target database have been updated since the stated time and date, click **Refresh Database Schemas**.
6. Select the sensitive type that best describes the sensitive columns that you want to add to your sensitive data model.
7. Find sensitive columns by entering or selecting one or more of the following items, and then click **Search**:
   - **Schema name**
   - **Table name**
   - **Column name**

   A list of sensitive columns that match your selection criteria are displayed.
8. Optional: Change the sensitive type of a column by selecting a new sensitive type from the **Sensitive Type** column.
9. Select the columns that you want to add to your sensitive data model, and then click **Add Columns**.

   To select all the columns, select the check box next to the **Schema** column heading. The columns are added to the sensitive data model and the sensitive data model is automatically saved.

Add Previously Removed Columns to a Sensitive Data Model

You can view the list of previously removed columns from a sensitive data model (SDM) and add those columns back to the SDM as needed.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.

   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model to which you want to add columns.
4. Scroll down to the **Sensitive Columns** list and click **View/Add Previously Removed Columns**.

   The **Add Previously Removed Columns** window is displayed. It shows a list of the schema, table, column, and data type for each previously removed column.
5. If you wish to add one or more columns back to the sensitive data model, select either
   - **Select specific columns** or
   - **All columns**
6. If you selected **Select Specific Columns** then choose the columns to add back from the list.
7. Click **Add Columns to Sensitive Data Model**.

Remove Sensitive Columns from a Sensitive Data Model

Sometimes Data Discovery returns columns that you do not want to include in your sensitive data model. You can remove them from the sensitive data model on the sensitive data model's page.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.

   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model from which you want to remove sensitive columns.
4. To remove a singular column, click the symbol to the right of **Sensitive Column** to be removed in the **Sensitive Columns** list.
   a. Click the **Remove** option.
   b. Click **Remove Column** in the dialog box to confirm the removal of the column.
5. To remove multiple columns, click **Remove Columns** above the **Sensitive Columns** list. The **Remove Columns** window is displayed.
   a. (Optional) Select a sensitive type that best describes the sensitive columns that you want to remove.
   b. Enter or select one or more of the following items, and then click **Search**:
      - **Schema name**
      - **Table name**
      - **Column name**

      A list of sensitive columns that match your selection criteria are displayed.
   c. Select the columns that you want to remove from your sensitive data model, and then click **Remove Columns**.

      To select all the columns, select the check box next to the **Schema** column heading. The columns are removed from the sensitive data model and the sensitive data model is automatically saved.

Update Sensitive Type for a Sensitive Column

Learn how to change the sensitive type of a sensitive column directly from the sensitive data model.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.

   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model from which you want to remove sensitive columns.
4. To update the sensitive type of a sensitive column, click the symbol to the right of **Sensitive Column** to be removed in the **Sensitive Columns** list.
5. Click the **Change Sensitive Type** option.

   The **Change Sensitive Type** dialog will appear.

6. Select the new **Sensitive Type** from the list.
   - (Optional) Change the compartment by clicking **Change Compartment** and selecting the appropriate compartment. This will allow you to view custom sensitive types from that compartment.
7. Click **Change Sensitive Type** button at the bottom of the dialog to finish changing the sensitive type of a sensitive column in a sensitive data model.

Add or Remove a Referential Relationship from a Sensitive Data Model

You can add or remove a referential relationship between database columns in your sensitive data model.

Referential relationships are leveraged in operations such as masking. During masking, the relationship helps ensure the integrity and consistency of the masking format applied. Relationships can also potentially be leveraged during incremental discovery using the sensitive data model (or manual column addition to the sensitive data model) to pull in other related columns.

Add Referential Relationship

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model for which you want to manage referential relationships.
4. Under **Resources**, click **Referential relationships.**
5. Click **Add referential relationship**.
6. Select if this referential relationship is either an **Application-level (non-dictionary) relation** or a **Database-level (dictionary-defined) relation**.
   You can manually enter referential relations, or they can be discovered through incremental discovery. See Perform an Incremental Discovery of Sensitive Data on Your Target Database for more information.

   > **Note:**
   >
   > If you manually enter a database-level relation, then is existence will be checked against the database.

7. In the **Choose parent column in sensitive data model** section, select the schema name, table name, and column name of the parent column in the relationship.
8. In the **Choose child column in sensitive data model** section, select the schema name, table name, and column name of the child column in the relationship.
9. Optionally, click **Add another column in composite relation** to add another column to the parent and child columns list to create a composite relationship mapping in Data Safe.
10. Select if you would like to either **Add columns to sensitive data model** or **Create referential relationship only**.
11. Optionally, select the **Sensitive type** for each column.
    Adding a sensitive type is only available if you are adding the referential relationship to the sensitive data model.

Selecting a sensitive type will ensure that the parent and child column get masked using the same masking format as both columns will be added to the sensitive data model with as the same sensitive type. If no sensitive type is provided, then the sensitive type of the parent column will be used in the child column as well.

However, if you have entered multiple columns to create a composite relationship, a new masking format will be created following a naming convention of `schema.parenttable.datetime`. This `schema.parenttable.datetime` masking format will automatically apply group masking with shuffle format when a masking job is initiated. See Group Masking Example Using Shuffle for more information.

12. Click **Add relationship**.

Delete a Referential Relationship

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
   A list of sensitive data models to which you have access is displayed.
3. Click the name of the sensitive data model for which you want to manage referential relationships.
4. Under **Resources**, click **Referential relationships.**
5. Select an application level referential relationship to delete from the table.

> **Note:**
>
> Database-defined relations can't be deleted.

   Additionally, you can only select one relationship to delete at a time.
6. Click **Delete referential relationship**.

Download or Upload a Sensitive Data Model in XML Format

You can download an XML version of a sensitive data model and upload it into Oracle Data Safe, replacing an existing sensitive data model or creating a new one. Before downloading a sensitive data model, you first need to generate it as an XML file.

About Downloading and Uploading Sensitive Data Models

There are several use cases for downloading and uploading sensitive data models, for example:

- You have multiple test databases in different regions in Oracle Cloud Infrastructure, all with the same schemas, and you want to use the same sensitive data model for them all.
- Your test database has moved to another region in Oracle Cloud Infrastructure and you want to move the sensitive data model with it.
- Your sensitive data model is large and complex so you prefer to manually edit the sensitive columns in a text editor instead of going through the Oracle Data Safe interface.

Generate a Sensitive Data Model

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. **Under List Scope**, select the compartment for your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.
   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.
   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. Click **Generate SDM**.

   The **Generate Sensitive Data Model for Download** dialog box is displayed.
7. Click **Generate SDM** and wait for the XML file to be generated.

   When the XML file is generated, a message states that the XML file generation is complete. You can download it using the **Download SDM** button.
8. Click **Close**.

Download a Sensitive Data Model

After you generate an XML version of your sensitive data model, you can download it to your local computer.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment for your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.
   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.
   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. Click **Download SDM**.

In some browsers, the file is directly downloaded to the local download folder. In others, the **Download Sensitive Data Model** dialog box is displayed and you must complete the following steps.

7. Click **Download SDM**.

   The **Opening SDM-download.xml** dialog box is displayed.

8. Leave **Save File** selected, and click **OK**.

   The **Enter name of file to save to** dialog box is displayed.

9. Browse to the location where you want to save the file, enter a file name in the **File name** box, and then click **Save**.

Upload a Sensitive Data Model

You can upload a sensitive data model in XML format into Oracle Data Safe. During the import, you can choose to update an existing sensitive data model or create a new one. When creating a new one, you need to select the target database to which the sensitive data model applies.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Click **Upload Sensitive Data Model**.

   The **Upload Sensitive Data Model** window is displayed.

4. To replace an existing sensitive data model, do the following:
   a. Leave the **Update an existing sensitive data model** tile selected.
   b. Select the sensitive data model that you want to replace. If needed, click **Change Compartment** and select a different compartment.
   c. Add your sensitive data model. There are two ways to do this. The first way is to drag your sensitive data model file (XML file) onto the **Upload Sensitive Data Model File** area. The second way is to click **select one**, browse to and select your XML file in the **File Upload** dialog box, and then click **Open**.
   d. Click **Upload Sensitive Data Model**.
5. To create a new sensitive data model, do the following:
   a. Select the **Create a new sensitive data model** tile.
   b. Enter a name for your new sensitive data model.
   c. Select the compartment in which you want to store your sensitive data model.
   d. (Optional) Enter a description for your sensitive data model.
   e. Select the target database to which your sensitive data model applies.
   f. Add your sensitive data model. There are two ways to do this. The first way is to drag your sensitive data model file (XML file) onto the **Upload Sensitive Data Model File** area. The second way is to click **select one**, browse to and select your XML file in the **File Upload** dialog box, and then click **Open**.
   g. (Optional) To add tags, click **Show Advanced Options**, and create tags.
   h. Click **Upload Sensitive Data Model**.

      It's important to leave the window open during the upload process.

Manage Sensitive Data Models

You can manage sensitive data models.

Move a Sensitive Data Model to a Different Compartment

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment that contains your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.
   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.
   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. From the **More Actions** menu, select **Move Resource**.

   The **Move Resource to a Different Compartment** dialog box is displayed.
7. Select a compartment, and then click **Move Resource**.

   The sensitive data model is moved immediately.

Change the Target Database Associated with a Sensitive Data Model

You can change the target database associated with a sensitive data model. All operations, such as performing data discovery and adding columns manually, are done in context of the associated target database. Changing the target database does not perform data discovery or update the sensitive data model in any way. It may result in stale information in the sensitive data model. Oracle recommends that after you change the target database you perform incremental data discovery to check the differences between your sensitive data model and the new target database.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment that contains your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.

c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.

d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.

e. Click **Apply Filters**.

5. Click the name of your sensitive data model to view its details.
6. On the **Sensitive Data Model Information** tab, click **Edit** next to the target database name.

   The **Change Target Database** dialog box is displayed.
7. Select a different target database. If needed, click **Change Compartment** and select a different compartment.
8. Click **Submit**.

Delete a Sensitive Data Model

Deleting a sensitive data model is permanent. If you want a backup copy of your sensitive data model before deleting it, you can generate an XML version of it and download it beforehand.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment that contains your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:

   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).

   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.

   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.

   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.

   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. From the **More Actions** menu, select **Delete**.

   The **Delete Sensitive Data Model** dialog box is displayed.
7. If you are sure that you want to delete your sensitive data model, click **Delete**.

   The sensitive data model is deleted immediately.

Download Data Discovery Reports

You can download a report about a sensitive data model or the latest incremental discovery for a sensitive data model. Before downloading a report, you first need to generate it. PDF and XLS file formats are available.

About Data Discovery Reports

The Sensitive Data Model report contains information about all the sensitive columns in the sensitive data model. The Latest Incremental Discovery report contains information only about the sensitive columns that were discovered after the sensitive data model was generated. Both include the following information:

- The name of the sensitive data model
- The name of the target database associated with the sensitive data model
- The date and time the report was generated
- The total number of columns and values scanned
- The total number of discovered sensitive types, sensitive tables, sensitive columns, and sensitive values
- (For each sensitive column) The sensitive type, schema name, table name, and column name
- (For each sensitive column) The sensitive value count, whether the column data was matched (Y or N), whether the column name was matched (Y or N), and whether the column comment was matched (Y or N)

Generate a Data Discovery Report

Generate the report that you want to download.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment that contains your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.
   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.
   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. Click **Generate Report**.

   The **Generate Report** dialog box is displayed.
7. Select the type of report that you want to generate: **Sensitive Data Model** or **Latest Incremental Discovery**.
8. Select the report format: **PDF** or **XLS**.
9. Click **Generate Report** and wait for a message that says the report generation is complete.

10. Click **Close**.

Download a Data Discovery Report

After you generate a report, you can open it or download it to your local computer.

1. Under **Security Center**, click **Data Discovery**.
2. Under **Related Resources**, click **Sensitive Data Models**.
3. Under **List Scope**, select the compartment that contains your sensitive data model.
4. To filter the list of sensitive data models, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any State**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) To search by target databases: Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Sensitive data model name** box, enter the full name (it's case sensitive) of the sensitive data model name.
   d. (Optional) To search by date/time: In the **Time created before** box, click the calendar widget, and configure the year/month/day.
   e. Click **Apply Filters**.
5. Click the name of your sensitive data model to view its details.
6. Click **Download Report**.

   The **Download Report** dialog box is displayed.
7. Select the type of report that you want to download: **Sensitive Data Model** or **Latest Incremental Discovery**.
8. Select the report format: **PDF** or **XLS**.
9. Click **Download Report** and wait for a message that says the report download is complete.
10. Click **Download Report**.

    In some browsers, the report is directly downloaded to your local download folder and the operation is complete. In others, a dialog box is displayed with options to open the report or save it to your local computer as in the following steps.
11. If you want to view the report, do the following:
    a. Select **Open with**.
    b. Select an application that can open the PDF or XLS file.
    c. Click **OK**.

       The report is displayed in the selected application.
12. If you want to save the report to your local computer, do the following:
    a. Select **Save File**.
    b. Click **OK**.
    c. Browse to the location on your local computer to where you want to save the file, enter a file name, and then click **Save**.

Create and Modify Event Notifications in Data Discovery

You can create and modify event notifications in Data Discovery.

Creating Event Notifications for Data Discovery

In Data Safe you can create event notifications for Data Discovery related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.
6. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Data Discovery Event Types in the *Administering Oracle Data Safe* guide for more information on events.
7. Select to either **Create new topic** or to **Select existing topic**.
8. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

9. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
10. Select a **Subscription protocol**.
11. Provide the necessary inputs for the selected subscription protocol.
12. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
13. Click **Create notification**.

Modifying Event Notifications For Data Discovery

After creating event notifications in Data Discovery in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
3. Click the **Notifications** tab.
4. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

7

Data Masking

This section discusses how to mask sensitive data in non-production databases by using the Data Masking feature in Oracle Data Safe.

Data Masking Overview

Data masking is the process of permanently replacing sensitive data with fictitious yet realistic looking data to protect confidential information.

The Challenge

The amount of data that organizations collect and manage, including sensitive and personal data, is growing every day. The growing security threats have made it necessary to limit exposure of sensitive data. At the same time, different data privacy laws and standards such as EU GDPR, PCI-DSS, and HIPPA mandate you to protect personal data. Live production database environments contain valuable and sensitive data, and to meet security and compliance requirements, you need to protect this data. Usually, organizations implement multiple security controls in their production environments to ensure that access to sensitive data is tightly controlled.

You collect data probably to improve your products and services, provide better user experience, and support and grow your business. To best utilize the collected data, you need to share it with different teams, both internal and external, for various use-cases such as development, testing, training, and data analytics. Copying production data for non-production purposes proliferates sensitive data, expands the security and compliance boundary, and increases the likelihood of data breaches. If left unprotected, contractors or offshore workers might access the data and possibly move it across locations. Data privacy standards such as PCI-DSS and EU GDPR also emphasize on protecting sensitive information in non-production environments because these environments are typically not as protected or monitored as production systems.

The challenge is to reduce the unnecessary spread and exposure of sensitive data while maintaining its usability for non-production purposes.

The Solution

Even in non-production environments, you need to protect your sensitive data and stay compliant with data privacy regulations. The recommended solution is to mask your sensitive data before using it in non-production environments. This way, you minimize the sensitive data you have, and thus, reduce the risk and compliance boundary.

Data masking, also known as static data masking, is the process of permanently replacing sensitive data with fictitious yet realistic looking data. It helps you generate realistic and fully functional data with similar characteristics as the original data to replace sensitive or confidential information. Data masking limits sensitive data proliferation by anonymizing sensitive data while enabling you to use production-like data. It ensures that malicious actors cannot benefit from the fictitious data even if they gain access to it.

Data masking is ideal for virtually any situation when confidential or regulated data needs to be shared with non-production users. These users may include internal users, such as application developers or external business partners, such as offshore testing companies, suppliers, and customers. Data masking contrasts with encryption, which simply hides data, and the original data can be retrieved with the appropriate access or key. With data masking, the original sensitive data cannot be retrieved or accessed.

One of the key aspects of data masking is to replace sensitive information with fictitious data, without breaking the semantics and structure of the data. The masked data must be realistic and pass specific checks, such as Luhn validation. For example, a masked credit card number must not only be a valid credit card number, but also a valid Visa, Mastercard, American Express, or Discover card number. Failing to maintain this data integrity may break the corresponding application. The predefined masking formats ensure that the generated data passes common validation checks.

Common Data Masking Requirements

Organizations typically mask data using custom scripts or solutions. While these in-house solutions might work for a few columns, they do not work for large applications with distributed databases and thousands of columns. An enterprise data masking solution should be able to fulfill the following data masking requirements:

- Locate sensitive data in the midst of numerous applications, databases, and environments.
- Correctly mask sensitive data having different shapes and forms such as names, Social Security numbers, email addresses, credit card numbers (Mastercard, Visa, and so on), and blood type.
- Ensure that the masked data is irreversible, that is, one should not be able to retrieve the original data from the masked data.
- Ensure that the masked data is realistic enough to be useful for non-production purposes such as development and analytics.
- Ensure that the applications continue to work with the masked data.

Data Masking in Oracle Data Safe

The Data Masking feature in Oracle Data Safe addresses the common data masking requirements and more. It simplifies the process of masking data in your non-production databases by providing an automated, flexible, and easy-to-use solution. It enables you to:

- Maximize the business value of your data without exposing the sensitive data
- Minimize the compliance boundary by not proliferating the sensitive production data
- Mask your Oracle databases
- Use various masking techniques to meet your specific business requirements
- Preserve data integrity ensuring that the masked data continues to work with applications

Masking Policies and Masking Formats

By using Data Discovery and Data Masking in Oracle Data Safe, you can mask the sensitive data in your target databases. Data Discovery lets you discover sensitive data and referential (parent-child) relationships in a target database, and generate a sensitive data model containing all the sensitive columns and metadata. Data Masking lets you create a masking

policy for the sensitive data model and then apply that policy against a target database to mask its sensitive data. Data masking ensures referential integrity by masking related columns consistently.

When creating a masking policy, you select a masking format for each sensitive column in the sensitive data model. A masking format defines the logic to mask data in a database column. Oracle Data Safe automatically selects a default predefined masking format for each sensitive column for you, however, you can change the selections as needed. Oracle Data Safe provides a comprehensive set of predefined masking formats for common sensitive and personal data, such as names, national identifiers, credit card numbers, phone numbers, and religion. For example, the Email Address masking format replaces values with random email addresses. You can also create your own masking formats, use conditional masking, and implement group masking.

One of the key aspects of data masking is to replace the sensitive information with fictitious data, without breaking the semantics and structure of the data. The masked data must be realistic and pass specific checks, such as Luhn validation. For example, a masked credit card number must not only be a valid credit card number, but also a valid Visa, Mastercard, American Express, or Discover card number. Failing to maintain this data integrity may break the corresponding application. The predefined masking formats ensure that the generated data passes common validation checks.

Similar to sensitive data models, Oracle Data Safe stores your masking policies and user-defined masking formats in compartments in Oracle Data Safe. You can move them from compartment to compartment and delete them as needed. To apply masking policies to target databases in different regions or to simply edit masking policies manually in a text editor, you can download and upload masking policies in XML format.

When configuring a data masking job, you have the option to upload scripts to be run on the target database before and/or after the data masking job. For example, you can upload a pre-masking script to create a column on the target database that should be used for the Deterministic Substitution masking format. And, you can upload a post-masking script to remove this column after data masking completes.

Characteristics of Masking Formats

Data masking formats have characteristics. Some common characteristics include combinable, uniqueness, reversible, and deterministic. Oracle Data Safe has a wide range of predefined and basic masking formats. Some masking formats support double-byte characters, for example, Japanese, other Asian, and Cyrillic characters.

Combinable

A masking format is considered *combinable* when it can be combined with other basic masking formats or predefined masking formats though the use of conditions.

For example, assume that you want to mask a column containing data in format `999-999`, where `9` signifies a digit. You want to replace the first three digits with a fixed three-digit number, preserve the hyphen, and replace the last three digits with some random digits. To generate the expected data, you could combine three basic masking formats: Fixed Number, Fixed String, and Random Number, as shown in the following example. The outputs of these

three masking formats are concatenated to generate the masked values, for example, `678-333`, `678-110`, `678-656`, and `678-999`.

```
FIXED NUMBER 678
FIXED STRING "-"
RANDOM NUMBER [START:100 END: 999]
```

Another example uses a basic masking format with a predefined masking format. Suppose you want to mask a social security number. The logic is: If a social security number exists, replace it with a predefined social security number. Otherwise, replace it with a random number.

Uniqueness

A masking format is characterized as having *uniqueness* if it ensures uniqueness of the generated masked data. These types of masking formats are useful for masking columns with uniqueness constraints. For example, you may want to mask a column of EMPLOYEE IDs with unique ID masked values. No two rows can have the same ID.

Reversible

A masking format that is characterized as *reversible* can retrieve original column data from masked data. Data masking usually means permanently replacing the data and ensuring that no one can retrieve the original data. But, sometimes you might want to see the original data. Reversible masking is helpful when businesses need to mask and send their data to a third party for analysis, reporting, or any other business processing purpose. After the processed data is received from the third party, the original data can be recovered. The Deterministic Encryption masking format supports reversible masking.

Deterministic

One of the key requirements for masking data in large databases or multiple database environments is to mask some data consistently. That is, for a given input, the output should always be the same. At the same time, the masked output should not be predictable. A *deterministic* masking format generates consistent output for a given input across databases and data masking jobs. Deterministic masking helps to maintain data integrity across multiple applications and preserve system integrity in a single sign-on environment.

For example, consider three applications: a human capital management application, a customer relationship management application, and a sales data warehouse. These three applications may have key common fields such as `EMPLOYEE_ID` that must be masked consistently across these applications. Deterministic masking techniques can be used here to ensure consistency.

Let's consider another example. Suppose that two values, Joe and Tom, are masked to Henry and Peter by using a deterministic masking technique. When you repeat the technique on another database, Bob and Tom (if they exist), might be replaced with Louise and Peter. Notice that even though the two runs have different data, Tom is always replaced with Peter.

The Deterministic Encryption, Deterministic Substitution, SQL Expression, and User Defined Function masking formats support deterministic masking.

Characteristics of Each Data Masking Formats

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Age	Number - Not Applicable	No	Yes	No	No	No
Australian Business Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Australian Company Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Australian Medicare Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Australian Medicare Provider Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Australian Tax File Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Bank Account Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Bank Routing Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Blood Type	No	No	Yes	No	No	No
Canada Postal Code	No	No	Yes	No	No	No
Canada Social Insurance Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Canada Social Insurance Number (hyphenated)	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
China Resident ID (PRC) Number	Number - Not Applicable	No	Yes	No	No	No
Credit Card Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Credit Card Number (Type and Format Preserving)	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Credit Card Number-American Express	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Credit Card Number-Discover	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Credit Card Number-Mastercard	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Credit Card Number-Visa	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Date-Card Expiration	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Date-Past	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Delete Rows	Number - Not Applicable	No	No	Not Applicable	No	Not Applicable
Deterministic Encryption Date	Yes	No	No	Yes	Yes	Yes. Refer to the Inputs section to see specific conditions.
Deterministic Substitution	Yes	No	No	Yes, as long as the values in the substitution column do not change and you provide the same seed value	No	No
Email Address	No	No	Yes	No	No	No
Finland Personal Identity Code	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Fixed Number	Number - Not Applicable	Yes	Yes	Yes	No	No
Fixed String	Yes	Yes	Yes	Yes	No	No
Format Preserving Randomization	No	No	Yes	No	No	No
Gender	No	No	Yes	No	No	No

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Group Shuffle	Yes	No	No	No	No	Yes, this masking format ensures uniqueness for columns that have unique constraints
Height (Centimeter)	Number - Not Applicable	No	Yes	No	No	No
IBAN	Alphanumeric - Not Applicable	No	Yes	No	No	No
IBAN (Hyphenated)	Alphanumeric - Not Applicable	No	Yes	No	No	No
ICD-9-CM	Alphanumeric - Not Applicable	No	Yes	No	No	No
ICD-10-CM	Alphanumeric - Not Applicable	No	Yes	No	No	No
Identification Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
IFSC Code	Alphanumeric - Not Applicable	No	Yes	No	No	No
IMEI Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Income	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
IPv4	Number - Not Applicable	No	Yes	No	No	No
IPv6	Alphanumeric - Not Applicable	No	Yes	No	No	No
IPv6 dual	Alphanumeric - Not Applicable	No	Yes	No	No	No
Japan My Number	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Korea Resident Registration Number (RRN)	Number - Not Applicable	No	Yes	No	No	No
Mac Address (Colon-Separated)	Number - Not Applicable	No	Yes	No	No	No
Mac Address (Dot-Separated)	Number - Not Applicable	No	Yes	No	No	No
Mac Address (Hyphenated)	Number - Not Applicable	No	Yes	No	No	No
Marital Status	No	No	Yes	No	No	No

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Mexico Company RFC ID	Alphanumeric - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Mexico CURP Code	Alphanumeric - Not Applicable	No	Yes	No	No	No
Mexico Individual RFC ID	Alphanumeric - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Netherlands Citizen Service Number (BSN)	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Null Value	Number - Not Applicable	Yes	No	Yes	No	No
Pattern Masking	No	No	No	No	No	No
Post Processing Function	Yes	No	Yes	Not Applicable	Not Applicable	Not Applicable
Preserver Original Data	Yes	No	No	Yes	Not Applicable	If the original values are unique, they will remain unique after masking
Race	No	No	Yes	No	No	No

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Random Date	Number - Not Applicable	No	Yes	No	No	Yes. The total number of distinct values in the specified range must be greater than or equal to the number of values in the column
Random Decimal Number	Number - Not Applicable	No	Yes	No	No	Yes. The total number of distinct values in the specified range must be greater than or equal to the number of values in the column
Random Digits	Number - Not Applicable	No	Yes	No	No	Yes, however, if you do not specify a sufficient length range, you can run out of unique values within the range
Random List	Yes	No	Yes	No	No	Yes. The input list must have unique values, and the number of values in the list must be greater than or equal to the number of values in the column to be masked.

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Random Name	No	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Random Number	Number - Not Applicable	No	Yes	No	No	Yes. The number of distinct values in the specified range must be greater than or equal to the number of values in the column
Random String	No	No	Yes	No	No	Yes. The number of distinct values in the specified range must be greater than or equal to the number of values in the column
Random Substitution	Yes	No	No	No	No	Yes. The number of distinct values in the substitution column must be greater than or equal to the number of values in the column to be masked

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Regular Expression	Yes	Yes - Character (CLOB) and National Character (NCLOB) only	No	No	No	No
Religion	No	No	Yes	No	No	No
Sexual Orientation	No	No	Yes	No	No	No
Shuffle	Yes	No	No	No	No	Yes, provided the column values are all unique
SQL Expression	Y, the SQL expression provided should generate multi byte chars	Yes	No	Yes, depending on the SQL expression defined	No	Yes, but the uniqueness is not guaranteed and depends on the SQL expression defined. However, because ORA_HASH uses a 32-bit algorithm, and considering the birthday paradox or pigeonhole principle, there is a 0.5 probability of collision after 232-1 unique values.
Stock	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
Substring	Yes	No	Yes	Yes	No	No
SWIFT/BIC Code (11-digit)	Alphanumeric - Not Applicable	No	Yes	No	No	No

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
SWIFT/BIC Code (8-digit)	Alphanumeric - Not Applicable	No	Yes	No	No	No
Truncate Data	Yes	No	No	Not Applicable	Not Applicable	Not Applicable
UK National Insurance Number (Format-Preserving)	Alphanumeric - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	No
UK National Insurance Number (Space-Separated)	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
UK Postal Code (Space-Separated)	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
URL	No	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
US DEA Number	Alphanumeric - Not Applicable	No	Yes	No	No	No

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
US Phone Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
US Phone Number (With Country Code)	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
US Social Security Number	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
US Social Security Number (Hyphenated)	Number - Not Applicable	No	Yes, if the generated masked values passes the post processing function validation	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column
User Defined Function	Yes	No	Yes	Yes, depending on the function defined	No	Yes, depending on the function defined

Masking Format	Supports Double-Byte Characters*	Supports Large Object Columns	Combinable	Deterministic	Reversible	Uniqueness
Vehicle ID Number (VIN)	Alphanumeric - Not Applicable	No	Yes	No	No	No
Weight (Pound)	Number - Not Applicable	No	Yes	No	No	Yes, if the number of distinct values that can be generated by the LMF is greater than the number of distinct values in the column

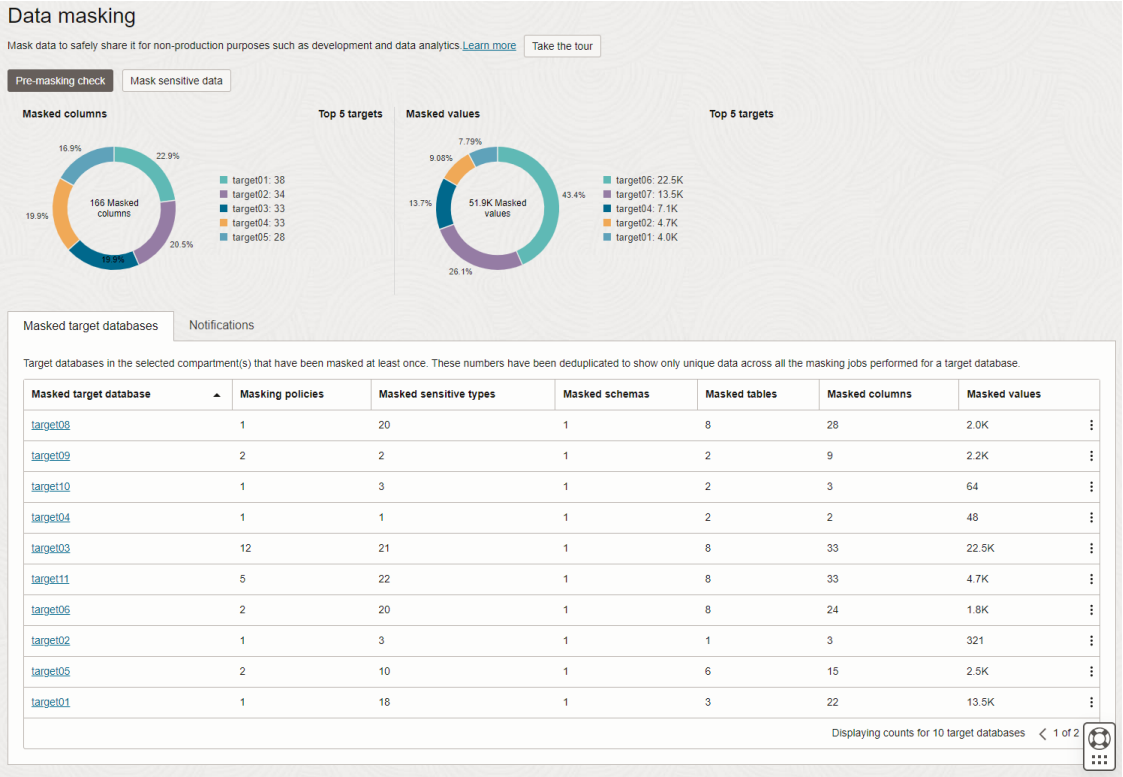
*If a masking format supports double-byte characters then you can use it for characters from languages such as Japanese, Chinese, and Cyrillic.

Data Masking Dashboard

The Data Masking dashboard, as shown below, provides a high-level view of your masked target databases in your selected compartment(s). The two charts at the top of the dashboard focus on your top five target databases. The first chart helps you to identify which target databases have the most masked columns by showing you a percentage breakdown of masked columns across the five targets. The second chart helps you to identify which target databases contain the most masked values by showing you a percentage breakdown of masked values across the five targets.

The table below the charts shows statistics about the target databases in the selected compartment(s). Each target database listed must have been masked at least once. You can view the number of masking policies created for each target database, the number of masked sensitive types, masked schemas, masked tables, masked columns, and masked values on each target database.

You can explore key features and workflows with the guided tour option by clicking the "Take the tour" button in the Data Masking dashboard.



Masked target databases

The **Masked target databases** tab shows you the target databases in the selected compartment(s) that have been masked at least once. You can click a target database name to view a masking summary for just that target database and details about its masking policies.

Notifications

The **Notifications** tab shows you what event notifications and subscriptions you have created for Data masking. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show Events that you have created directly within Data Safe. In addition to displaying existing event notifications, you can also create new notifications by using the **Create notification** button. See Create and Modify Event Notifications in Data Masking for more information.

Data Masking Workflow

Oracle recommends that you use the following approach and workflow to mask sensitive data with Oracle Data Safe.

1. **Important:** Create a backup of your production database. For example, you can use Recovery Manager (RMAN) and Oracle Cloud Storage service (or any other backup location) to create and store your production backups. You never want to mask the actual production database.
2. Clone the backup of your production database to create a stage database. Do not expose the stage database to users. Create the stage database on the Oracle Cloud with supported services.
3. Register your stage database withOracle Data Safe.

4. Use Data Discovery to discover sensitive data on the stage database and generate a sensitive data model.
5. Use Data Masking to create new masking formats if you require masking formats other than the Oracle predefined ones.
6. Use Data Masking to create a masking policy that associates default masking formats with the sensitive columns. You can change the formats as needed.
7. Run a Pre-Masking Check on your stage database to check if it is ready for masking. Perform any remediation recommendations prior to initiating a masking job.
8. Run a data masking job against your stage database to mask the sensitive data using the masking policy. Oracle Data Safe also generates a data masking report that shows you the results of your data masking job.
9. Verify the masked data by reviewing the Data Masking report and by validating the masked data.
10. Clone the stage database to create a test database. Or, export the masked data from the stage database, create a test database, and then import the masked data into the test database. Oracle strongly recommends creating a test database instead of giving your test and developer users access to your stage database.
11. Grant your test and developer users access to your test database.
12. Set up event notifications. For example, you can subscribe to the `Masking Job Begin` event to be automatically informed if a masking job is initiated.

Prerequisites for Using Data Masking

These are the prerequisites for using Data Masking:

- **Register the target databases that you want to use with Data Masking.**
- **Grant the Data Masking role on the target database.** A Database Administrator can grant this role to the Oracle Data Safe Service Account on the target database.
- **Obtain permission in Oracle Cloud Infrastructure Identity and Access Management (IAM) to use the Data Masking feature in Oracle Data Safe.** An OCI administrator can grant these permissions. These resources require permissions:
  - `data-safe-masking-policies`
  - `data-safe-library-masking-formats`
  - `data-safe-masking-reports`
    In order to perform data masking a user will need `manage` permissions on `data-safe-masking-reports` in the compartment of the target database.
  - `data-safe-masking-policy-health-report`
  - `data-safe-work-requests`

As an alternative to selectively granting permissions, you can grant permissions on `data-safe-masking-family` in the relevant compartments, which would include permissions on all of the resources above. See data-safe-masking-family Resource in the *Administering Oracle Data Safe* guide for more information.

Predefined Masking Formats

To help you mask common sensitive and personal data, such as credit card numbers, phone numbers, and national identifiers, Oracle Data Safe provides predefined masking formats. You can use predefined masking formats as is without providing any input. You cannot edit or delete predefined masking formats.

The following table describes the predefined masking formats.

Masking Format	Description
Age	Replaces values with random numbers from 0 through 110 **Examples:** • 18 • 75 • 102
Australian Business Number	Replaces values with random Australian business numbers. Ensures that the values pass the check test. **Examples:** • 66 325 112 895 • 72 435 134 666 • 93 832 434 258
Australian Company Number	Replaces values with random Australian company numbers. Ensures that the values pass the check test. **Examples:** • 004 499 987 • 010 749 961 • 945 382 463
Australian Medicare Number	Replaces values with random Australian medicare numbers. Ensures that the values pass the check test. **Examples:** • 2453 16245 1 • 4251 32340 0 • 6632 51126 1
Australian Medicare Provider Number	Replaces values with random Australian medicare provider numbers. Ensures that the values pass the check character test. **Examples:** • 4024742F • 6235441W • 8530682J
Australian Tax File Numbers	Replaces values with random Australian tax file numbers. Ensures that the values pass the check test. **Examples:** • 87653210 • 123456782 • 538273213
Bank Account Number	Replaces values with random 9 to 16-digit numbers **Examples:** • 7411024398 • 392663014671 • 24914700572445

Masking Format	Description
Bank Routing Number	Replaces values with random bank routing numbers. Ensures that the routing numbers pass the checksum test. **Examples:** • `121122676` • `322271627` • `061000052`
Blood Type	Replaces column data with values picked randomly from the following list: • A+ • A- • B+ • B- • AB+ • AB- • O+ • O-
Canada Postal Code (Space-Separated)	Replaces values with random Canada postal codes, which are in `A9A A9A` format, where `A` signifies a letter and `9` signifies a digit **Examples:** • `T7S T3R` • `J0L G6L` • `E4B L0V` **Details:** First character: • Randomly picks letters from A to Z except D, F, I, O, Q, U, W, and Z Second character: • Randomly picks digits from 0 to 9 Third character: • Randomly picks letters from A to Z except D, F, I, O, Q, and U Fourth character: • Space Fifth character: • Randomly picks letters from A to Z except D, F, I, O, Q, and U Sixth character: • Randomly picks digits from 0 to 9 Seventh character: • Randomly picks letters from A to Z except D, F, I, O, Q, and U
Canada Social Insurance Number	Replaces values with random Canada Social Insurance Numbers. Ensures that the numbers pass the Luhn's validation. **Examples:** • `688637008` • `346612823` • `734411531`

Masking Format	Description
Canada Social Insurance Number (Hyphenated)	Replaces values with random Canada Social Insurance Numbers, which are in 999-999-999 format, where 9 signifies a digit. Ensures that the numbers pass the Luhn validation. **Examples:** • 688-637-008 • 346-612-823 • 734-411-531
China Resident ID (PRC) Number	Replaces values with random China Resident ID numbers. Resident ID numbers are in 18-character structure with 17 digits and one alphanumeric character. **Examples:** • 618805200209090074 • 25675120140313003X • 169666197511150121
Credit Card Number	Replaces values with random credit card numbers. Generates card numbers of types: American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa. Ensures that the numbers pass the Luhn validation. **Examples:** • 4485780314771620 • 6011867455059259 • 5253901798047025
Credit Card Number (Hyphenated)	Replaces values with random hyphenated credit card numbers. It generates card numbers of type: American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa. Ensures that the numbers pass the Luhn validation. **Examples:** • 4485-7803-1477-1620 • 6011-8674-5505-9259 • 5253-9017-9804-7025
Credit Card Number-American Express	Replaces values with random 15-digit American Express credit card numbers. Ensures that the numbers pass the Luhn validation. **Examples:** • 377428083214575 • 342545797384840 • 371449635398431
Credit Card Number-Discover	Replaces values with random 16-digit Discover credit card numbers. Ensures that the numbers pass the Luhn validation. **Examples:** • 6011174868103745 • 6011006830091113 • 6011326843007736
Credit Card Number-Mastercard	Replaces values with random 16-digit Mastercard credit card numbers. Ensures that the numbers pass the Luhn validation. **Examples:** • 5233316245315286 • 5171736663215508 • 5479143620815877

Masking Format	Description
Credit Card Number-Visa	Replaces values with random 16-digit Visa credit card numbers. Ensures that the numbers pass the Luhn validation. **Examples:** • `4929680877575125` • `4716403468935369` • `4532622699903274`
Date-Card Expiration	Replaces values with random dates between 2000 and present. Day is always the last day of the month. **Examples:** • `2008-02-29` • `2014-08-31` • `2018-04-30`
Date-Past	Replaces values with random dates from 1950 through to the present date **Examples:** • 1970-01-01 • 2001-08-05 • 2018-10-16
Email Address	Replaces values with random email addresses while preserving the number of periods, hyphens, and underscores before the address sign (`@`). Possible top-level domains are: `.com`, `.org`, `.net`, `.edu`, `.gov`, `.int`, `.us`, `.uk`, `.eu`, `.cn`, `.in`, `.ru`, `.jp`, and `.au`. **Examples:** • `samar@example.com` could become `svkrpw@dmsoen.org` • `mike.williams@gmail.com` could become `sbvtud.ramzonibt@terim.net` • `ross_amara@gatech.edu` could become `qcipp_pnjetya@nbreqgp.gov`

Masking Format	Description
Finland Personal Identity Code	Replaces values with random Finland Personal Identity Codes **Examples:** • `160811A0142` • `251017A561N` • `300399-888Y` **Details:** Day of Birth: • Generates random 2-digit numbers between 01 and 30 Month of Birth: • Generates random 2-digit numbers between 01 and 12 Year of Birth: • Generates random 2-digit numbers between 00 and 99 Century Identification Sign: • Randomly picks characters from +, -, or A Individual Number: • Generates random 3-digit numbers between 000 and 999 Checksum Character: • Randomly picks characters from 0 through 9 or from A through Z, except for G, I, O, Q, and Z Sanity Check: • Uses Post Processing Function to ensure validity of the generated Personal Identity Codes
Format Preserving Randomization	Randomizes values while preserving their length, the position of letters and digits, the case of letters, and the special characters **Examples:** • `AjHjK123#@` could become `SbVbU574#@` • `678-704-7862` could become `281-272-1795` • `!@#$` remains `!@#$`
Gender	Replaces column data with values picked randomly from the following list: • Male • Female • Other
Height (Centimeter)	Replaces values with random numbers from 45 cm through 200 cm. **Examples:** • `60` • `162` • `176`
IBAN	Replaces values with random valid International Bank Account Numbers. IBAN are in alphanumeric character structure with 15-34 characters depending on the country. **Examples:** • `DE89370400440532013000` • `GB29NWBK60161331926819` • `FR1420041010050500013M02606`

Masking Format	Description
IBAN (Hyphenated)	Replaces values with random valid International Bank Account Numbers that are hyphenated. IBAN are in alphanumeric character structure with 15-34 characters depending on the country. **Examples:** • DE89-3704-0044-0532-0130-00 • GB29-NWBK-6016-1331-9268-19 • FR14-2004-1010-0505-0001-3M02-606
ICD-9-CM	Replaces values with random ICD-9-CM Codes. International Classification of Diseases (ICD) code is used for classifying diseases. **Examples:** • 328.95 • 536 • 600.95
ICD-10-CM	Replaces values with random ICD-10-CM Codes. International Classification of Diseases (ICD) code is used for classifying diseases. **Examples:** • N1M.3JCM • E4S • S1H.690T
Identification Number	Replaces values with random numbers from 1 through 999,999 **Examples:** • 166050 • 9887 • 46803
IFSC Code	Replaces values with random valid IFSC Code. IFSC Code are in XXX0(X|9)(X|9)(X|9)(X|9)(X|9) format where X is a letter, 0 is the number and 9 is a digit **Examples:** • HDFC0003636 • SBIN0010508 • ICIC0000269
IMEI Number	Replaces values with random 15-digit IMEI numbers. Ensures that the numbers pass the Luhn validation. **Examples:** • 490154203237518 • 357805023984942 • 352066060926230
Income	Replaces values with random numbers from 30,000 through 999,999 **Examples:** • 75001 • 155000 • 700999
IPv4	Replaces values with random valid IPv4 addresses. IPv4 addresses are in X.X.X.X where X is a number between 0 and 255 **Examples:** • 17.26.91.2 • 186.58.207.8 • 55.58.29.23

Masking Format	Description
IPv6	Replaces values with random valid IPv6 addresses. IPv6 addresses are in `X:X:X:X:X:X:X:X` where X is hexadecimal value between 0 and FFFF **Examples:** • `2001:0DB8:85A3:0000:0000:8A2E:0370:7334` • `D5AE:7B35:74EE:5E9A:C2F5:667B:3567:E6E6` • `4C92:EE9C:E5A2:7230:2FAF:33CE:9C3E:2323`
IPv6 dual	Replaces values with random valid IPv6 dual addresses. IPv6 dual addresses (ipv6+ipv4) are in `y:y:y:y:y:y:x.x.x.x` where y is hexadecimal value between 0 and FFFF and x is between 0 and 255 **Examples:** • `9435:8316:23FD:2B6:9B40:6B6B:176.235.52.158` • `26E9:E8D9:1D68:2309:2062:9090:75.234.0.54` • `DF0C:F237:F442:E997:D9FE:7979:241.206.191.216`
Japan My Number	Replaces values with random space separated Japan Individual Numbers **Examples:** • `7236 6487 2376` • `1675 8399 2830` • `8426 9458 0492`
Korea Resident Registration Number (RRN)	Replaces values with random Korea Resident Registration numbers. Resident Registration numbers are in `999999-9999999` format, where 9 signifies a digit **Examples:** • `260429-1808049` • `810502-1247315` • `310803-1339475`
Mac Address (Colon-Separated)	Replaces values with random valid Mac addresses. Mac addresses are in `XX:XX:XX:XX:XX:XX` where X is hexadecimal value between 0 and F **Examples:** • `C7:29:FF:EE:33:33` • `08:3E:C1:81:FF:FF` • `29:78:35:4D:00:00`
Mac Address (Dot-Separated)	Replaces values with random valid Mac addresses. Mac addresses are in `XXXX.XXXX.XXXX` where X is hexadecimal value between 0 and F **Examples:** • `86E6.25AE.BEBE` • `EE1E.8761.4141` • `217C.3CD7.2727`
Mac Address (Hyphenated)	Replaces values with random valid Mac addresses. Mac addresses are in `XX-XX-XX-XX-XX-XX` where X is hexadecimal value between 0 and F **Examples:** • `CF-4C-74-42-C4-44` • `1E-D1-ED-DB-1D-DD` • `D8-9D-C9-9C-D9-99`
Marital Status	Replaces column data with values picked randomly from the list: Single, Married, Separated, Divorced, Remarried, and Widowed

Masking Format	Description
Mexico Company RFC ID	Replaces values with a 12-character structure with 3 letters, 6 digits, and 3 alphanumeric characters. **Examples:** • `GAH7706035K2` • `TRQ9003057Z9` • `MNL820622PQ4`
Mexico CURP Code	Replaces values with an 18-character structure with 4 letters, 6 digits, 6 letters, and 1 alphanumeric character and 1 digit. **Examples:** • `HALW950522XBSCLCN9` • `JOFX590113MTSKSK85` • `KATE530108XBCJJJN7`
Mexico Individual RFC ID	Replaces values with a 13-character structure with 4 letters, 6 digits, and 3 alphanumeric characters. **Examples:** • `ZXCV990430AB7` • `LOPM850921X1A` • `TRQN9003057Z9`
Netherlands Citizen Service Number (BSN)	Replaces values with 9-digit number with a variant of the elf proof checksum: the weighted sum `(9×A + 8×B + ... + 2×H - 1x I)` must be divisible by 11. **Examples:** • `706424608` • `234567893` • `575903041`
Race	Replaces column data with values picked randomly from the list: White, African American, Asian, American Indian, Alaska Native, Native Hawaiian, and Other Pacific Islander
Random Name	Replaces values with random letters of random length. Compatible with character type columns only. **Examples:** • `AjHjK123#@` could become `Sbvtud` • `Michael` could become `Ramzoni` • `Richard Williams` could become `Madpalvik`
Religion	Replaces column data with values picked randomly from the list: Christianity, Islam, Nonreligious, Hinduism, Buddhism, Sikhism, Jainism, Judaism, and Other
Sexual Orientation	Replaces column data with values picked randomly from the list: Heterosexual, Homosexual, Bisexual, and Asexual
Stock	Replaces values with random numbers from 100 through 9,999 **Examples:** • `1300` • `5499` • `9990`

Masking Format	Description
SWIFT/BIC Code (11-digit)	Replaces values with random valid SWIFT Code. Swift Code are in `XXXXXX(X|9)(X|9)(X|9)(X|9)(X|9)` where X is a letter and 9 is a digit **Examples:** • `ISUFUF8I665` • `DKFKFKB2DRY` • `LORSRS0CKN2`
SWIFT/BIC Code (8-digit)	Replaces values with random valid SWIFT Code. Swift Code are in `XXXXXX(X|9)(X|9)` where X is a letter and 9 is a digit and last three characters are optional **Examples:** • `TWJLJLAK` • `ODSESEC9` • `KGOTOTKA`
UK National Insurance Number (Format-Preserving)	Replaces values with random UK National Insurance numbers preserving their length and format (To be used for UK NINO data only) **Examples:** • `AA 69 94 50 A` • `ZR-50-16-33-A` • `EE 253753 D`
UK National Insurance Number (Space-Separated)	Replaces values with random UK National Insurance numbers, which are in AA 99 99 99 A format, where A signifies a letter and 9 a digit **Examples:** • `AA 69 94 50 A` • `ZR 50 16 33 A` • `EE 25 37 53 D` **Details:** First Prefix Letter • Randomly picks letters from A to Z except D, F, I, Q, U, and V Second Prefix Letter • Randomly picks letters from A to Z except D, F, I, Q, U, and V 6 Digits • Generates random 6-digit numbers Suffix Letter • Randomly picks letters from A to D Sanity Check and Formatting • Uses Post Processing Function to format and ensure validity of the generated National Insurance numbers

Masking Format	Description
UK Postal Code (Space-Separated)	Replaces values with random UK postal codes, which are in AA9A 9AA format, where A signifies a letter and 9 a digit **Examples:** • `SE1P 4SA` • `EC1A 1BB` • `SW1A 0AA` **Details:** First Character: • Randomly picks letters from A to Z except Q, V, and X Second Character: • Randomly picks letters from A to Z except I, J, and Z Third Character: • Randomly picks digits from 0 to 9 Fourth Character: • Randomly picks letters from A, B, E, H, M, N, P, R, V, W, X, and Y Fifth Character: • Space Sixth Character: • Randomly picks digits from 0 to 9 Seventh Character: • Randomly picks letters from A to Z except C, I, K, M, O, and V Eighth Character: • Randomly picks letters from A to Z except C, I, K, M, O, and V
URL	Replaces values with random URLs starting with `http` or `https`. Possible top-level domains are: `.com`, `.org`, `.net`, `.edu`, `.gov`, `.int`, `.us`, `.uk`, `.eu`, `.cn`, `.in`, `.ru`, `.jp`, and `.au`. **Examples:** • `https://www.hapiden.com` • `http://www.qazwsx937.gov` • `https://www.bhatag.in`
US DEA Number	Replaces values with random US DEA Numbers with a 9-character structure with 2 letters, 6 letters and 1 checksum digit. **Examples:** • `GS7763825` • `UX3042265` • `CE4323565`

Masking Format	Description
US Phone Number	Replaces values with random 10-digit US phone numbers **Examples:** • `6787047862` • `2025550149` • `5206625256` **Details:** Area Code: • Randomly picks 3-digit codes from 328 US area codes Remaining 7 Digits: • Generates random 7-digit numbers Sanity Check: • Uses Post Processing Function to ensure validity of the generated phone numbers
US Phone Number (With Country Code)	Replaces values with random US phone numbers, which are in +1 (999) 999-9999 format, where 9 signifies a digit **Examples:** • `+1 (678) 704-7862` • `+1 (202) 555-0149` • `+1 (520) 662-5256` **Details:** Country Code: • +1 Area Code: • Randomly picks 3-digit codes from 328 US area codes Remaining 7 Digits: • Generates random 7-digit numbers Sanity Check and Formatting: • Uses Post Processing Function to format and ensure validity of the generated phone numbers
US Social Security Number	Replaces values with random US Social Security numbers **Examples:** • `148923857` • `771182740` • `562998392`
US Social Security Number (Hyphenated)	Replaces values with random US Social Security numbers, which are in `999-99-9999` format, where `9` signifies a digit **Examples:** • `148-92-3857` • `771-18-2740` • `562-99-8392`
Vehicle ID Number (VIN)	Replaces values with random Vehicle ID Numbers. VINs are in 17 characters format, made up of alphanumeric characters. **Examples:** • `5DL6Z9096QDLZLDDD` • `LAXLRQV73A2O8X222` • `2WWHFLU6567BIW777`

Masking Format	Description
Weight (Pound)	Replaces values with random numbers from 5 through 250. The range covers weight in pounds. **Examples:** • 45 • 176 • 210

Basic Masking Formats

Oracle Data Safe supports several basic masking formats that you can use as building blocks when creating new masking formats.

Delete Rows

Purpose

The Delete Rows masking format deletes the rows that meet a user-specified condition. It is useful in conditional masking when you want to delete a subset of values in a column and mask the remaining values using some other masking formats. You should be careful while using this masking format. If no condition is specified, all rows in a table are deleted. If a column is being masked using Delete Rows, there must not be a foreign key constraint or dependent column referring to the table.

> **See Also:**
>
> Example 1: Protecting Sensitive Identifiers Across Diverse Geographic Regions

Inputs

- No inputs are required.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: No
- Deterministic: Does not apply
- Reversible: No
- Uniqueness: Does not apply

Example

Assume that a table has `EMPLOYEE_ID` and `SALARY` columns, and you want to delete the salary data for a subset of employee IDs. You can specify a condition on the `SALARY` column using `EMPLOYEE_ID` to delete rows matching the condition. You can use some other masking formats to mask the remaining salary values.

The logic to mask `SALARY` might look like the following:

```
EMPLOYEE_ID < 100
      DELETE ROWS
EMPLOYEE_ID < 200
      RANDOM NUMBER [Start Value:30000 End Value:500000]
DEFAULT
      PRESERVE ORIGINAL DATA
```

Deterministic Encryption

Purpose

The Deterministic Encryption masking format encrypts column data using a cryptographic key and Advanced Encryption Standard (AES 128). The format of the column data after encryption is similar to that of the original values. For example, if you mask nine-digit numbers, the encrypted values also have nine digits.

Deterministic Encryption is a deterministic and reversible masking format. It is helpful when businesses need to mask and send their data to a third party for analysis, reporting, or any other business processing purpose. After the processed data is received from the third party, the original data can be recovered (decrypted) using the same seed value that was used to encrypt the data.

> **Note:**
>
> Deterministic Encryption is not supported for Oracle Database 11.2.0.4.

Inputs

- **Regular Expression:** Provide a regular expression to mask a character or numeric column.

  For data with characters in the ASCII character set, providing a regular expression is optional. However, you need to provide a regular expression if the data contains multi-byte characters. If not provided, an error is returned when a multi-byte character is found.

  In the case of ASCII characters, if a regular expression is not provided, Deterministic Encryption can encrypt variable-length column values while preserving their original format.

  If a regular expression is provided, the column values in all the rows must match the regular expression. Deterministic Encryption supports a subset of the regular expression language. It supports encryption of fixed-length strings, and does not support * or + syntax of regular expressions. The encrypted values also match the regular expression, which helps to ensure that the original format is preserved. If an original value does not match the

regular expression, Deterministic Encryption might not produce a one-to-one mapping. All non-confirming values are mapped to a single encrypted value, thereby producing a many-to-one mapping.

Deterministic Encryption can encrypt column values with up to 27 characters. This limit excludes special characters. Also, the limit can be lower for multi-byte characters.

> **WARNING:**
>
> If you choose to encrypt without using a regular expression, the column values exceeding the length restriction still get masked, but you might not be able to decrypt them back properly. If a regular expression is provided, size estimation is done using the regular expression and an error is returned if the length restriction is exceeded.

- **Seed Value:** Deterministic Encryption uses a seed value to generate a cryptographic key for encryption and decryption. Provide the seed value at the time of submitting the data masking job. It can be any string containing alphanumeric characters.
- **Decrypt Option:** If your masking policy has a sensitive column using the Deterministic Encryption masking format, you are shown the decrypt option while submitting the data masking job. Choosing this option, you can decrypt the encrypted column values.
- **For Date types:** To mask a date type column, provide a start and end date. You can use the calendar widget to select the dates. The start date must be less than or equal to the end date.

  The column values in all the rows must be within the specified date range. The encrypted values are also within the specified range. Therefore, to ensure uniqueness, the total number of dates in the range must be greater than or equal to the number of distinct original values in the column. If an original value is not in the specified date range, Deterministic Encryption might not produce a one-to-one mapping. All non-confirming values are mapped to a single encrypted value, thereby producing a many-to-one mapping.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: Yes
- Reversible: Yes
- Uniqueness: Yes. Refer to the Inputs section to see specific conditions.

Example

Suppose you want to encrypt US Social Security numbers, such as 333-93-4245. You can simply choose Deterministic Encryption without providing a regular expression. It automatically encrypts the numbers while preserving the format.

If you want to restrict the characters in encrypted values, you can provide a regular expression. For example, you can use the regular expression `[1-8][0-9]{2}-[0-9]{2}-[0-9]{4}` if the first digit in your numbers is between 1 and 8, and you want to ensure the same in the encrypted values.

> **See Also:**
>
> Regular Expressions for help on writing regular expressions.

Deterministic Substitution

Purpose

The Deterministic Substitution masking format uses the specified substitution column as the source of masked values. It performs hash-based substitution to replace the original data in a column with values from the substitution column.

Inputs

- **Schema Name:** The name of the schema containing the substitution column
- **Table Name:** The name of the table containing the substitution column
- **Column name:** The name of the substitution column containing the data that should be used for masking. The data types of the specified substitution column and column being masked must be the same. The substitution column must be present and accessible on the target database before masking. You can also use a pre-masking script to create this column.
- **Seed value:** Deterministic Substitution uses a seed value to perform hash-based substitution. Provide the seed value at the time of submitting a data masking job. It can be any string containing alphanumeric characters. To perform deterministic masking, you need to use the same seed value across multiple masking runs.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: Yes, as long as the values in the substitution column do not change and you provide the same seed value
- Reversible: No
- Uniqueness: No

Example

Suppose you discover a sensitive column named `EMP_ID` that contains employee IDs. Let's assume that you have fake employee ID values stored in another column named `SUB_EMP_ID`,

which resides in the SUB_EMPLOYEES table in the SUB_HR schema. When configuring the masking policy in the Data Masking wizard, you choose the Deterministic Substitution masking format for the EMP_ID column and provide the inputs: SUB_HR, SUB_EMPLOYEES, and SUB_EMP_ID.

You also specify a seed value at job submission time. When the job runs, Data Masking replaces the values in the EMP_ID column with the fake values from the SUB_EMP_ID column. In the future, you can mask this column (or other similar columns) using the same substitution column and seed value to ensure that the employee IDs are masked the same way.

Fixed Number

Purpose

The Fixed Number masking format replaces column data with a user-specified fixed number.

Inputs

- **Fixed Number:** The number that should be used to replace the column values. It can be any integer or decimal number, including negative numbers. The specified number should be valid for the column size.

Supported Data Types

- Character
- Numeric
- Large Object (LOB)

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: Yes
- Deterministic: Yes
- Reversible: No
- Uniqueness: No

Examples

- Suppose you want to replace all the Social Security numbers in a column with 999999999. You can use the Fixed Number masking format and provide this number as input.
- Alternatively, you can combine multiple basic masking formats to mask a column value. For example, you can use the Fixed Number masking format to ensure that the masked value starts with 990. Then, you can use the Random Number masking format to randomly generate the remaining seven digits.

Fixed String

Purpose

The Fixed String masking format replaces column data with a user-specified fixed string.

Inputs

- **Fixed String:** The string that should be used to replace the column values. It should be valid for the column size.

Supported Data Types

- Character
- Large Object (LOB)

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: Yes
- Deterministic: Yes
- Reversible: No
- Uniqueness: No

Examples

- Suppose you want to replace all the Social Security numbers in a column with `***-**-****`. You can use the Fixed String masking format and provide this string as input.
- Alternatively, you can combine multiple basic masking formats to mask a column value. For example, you can use the Fixed String masking format to ensure that the masked value starts with `***-**-`. Then, you can use the Random Number masking format to randomly generate the remaining four digits.
- Similarly, you can use the Fixed String masking format to ensure that the license plate numbers in a column start with "CA."

Group Shuffle

Purpose

The Group Shuffle masking format enables you to randomly reorder (shuffle) column data within discrete units, or groups, where there is a relationship among the members of each group.

Inputs

- **Grouping Columns (Optional):** One or more reference columns that should be used to group the values in the column to be masked. The grouping columns and the column to be masked must belong to the same table.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes

- Combinable: No
- Deterministic: No
- Reversible: No
- Uniqueness: Yes, this masking format ensures uniqueness for columns that have unique constraints

Example

Suppose you have two groups of employees: managers (M) and workers (W). You want to shuffle all the salaries, but you do not want the salaries of the managers getting mixed into the salaries of the workers. You can use the Group Shuffle masking format to shuffle the `SALARY` column within each group, which is derived from the unique values in the `JOB_CATEGORY` column.

The following table illustrates a group shuffle on the `SALARY` column, where the `JOB_CATEGORY` column is the grouping column. The rows with `JOB_CATEGORY` = M belong to one group and the `SALARY` values belonging to this group are shuffled within the group. Similarly, the rows with `JOB_CATEGORY` = W belong to another group and the `SALARY` values belonging to this group are shuffled within the group.

EMPLOYEE	JOB_CATEGORY	SALARY	SHUFFLED_SALARY
Alice	M	90	88
Bill	M	88	90
Carol	W	72	70
Denise	W	57	45
Eddie	W	70	57
Frank	W	45	72

Null Value

Purpose

The Null Value masking format replaces column data with `NULL`. The column being masked must be allowed to contain null values.

Inputs

- No inputs are required.

Supported Data Types

- Character
- Numeric
- Date
- Large Object (LOB)

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: No

- Deterministic: Yes
- Reversible: No
- Uniqueness: No

Example

Suppose you have a column named `SALARY` that contains salary information and you want to replace those numbers with `NULL`. You can apply the Null Value masking format to the `SALARY` column.

Pattern Masking

Purpose

The pattern masking format generates masked data in a user-defined way. This simplified masking format ensures flexibility in defining the output format.

Inputs

Pattern: The input pattern defines how random values are generated within the masked data, allowing a maximum generated data length of 30 characters. It supports specific placeholders:

- `%c` for a random lowercase letter
- `%C` for a random uppercase letter
- `%u[]` for a random character from a user-defined set
- `%%` for a %
- `%d` for a random digit

Users can also specify `%nd`, `%nc`, `%nC`, or `%nu[]` to generate `n` random digits, letters, or characters from a given set, respectively, where n ranges from 0 to 9. For instance, `%3d` will generate three random digits or `%5C` will generate five random uppercase letters. See the examples below for more details.

Any other character in the pattern is retained as-is in the output.

Supported Data Types

Character

Characteristics

- Supports double-byte characters: No
- Combinable: No
- Deterministic: No
- Reversible: No
- Uniqueness: No

Examples

- Use the pattern `%3d-%5C` to generate data like `416-JQPCS`.
- Use the pattern `%3d-%5c` to generate data like `416-dehco`.

- Use the pattern `%u[$^#]` to generate data like `$`.
- Use the pattern `%%%3d` to generate data like `%704`.

Post Processing Function

Purpose

The Post Processing Function masking format is a special masking option that enables you to use a custom function to further transform column values after they have been masked using some other masking formats. It takes the intermediate masked values as input and returns the final masked values. For example, you can use it for adding checksums or special encodings to the masked values. This masking option requires some level of coding skills.

Inputs

- **Package Name (Optional):** The name of the database package
- **Function Name:** The name of the database function

The database function has a fixed signature:

```
function post_proc_func (rowid varchar2, column_name varchar2, mask_value
varchar2)
return varchar2;
```

where:

- `rowid` is the row identifier of the row containing the value to be masked.
- `column_name` is the name of the column to be masked.
- `mask_value` is the value to be masked.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: Yes
- Deterministic: Does not apply
- Reversible: Does not apply
- Uniqueness: Does not apply

Example

You can use Post Processing Function to add a comma or dollar sign to a value. Suppose that you mask a `SALARY` column by using the Random Number masking format. You can then apply

the Post Processing Function masking format to the masked values to add a currency symbol, such as `$`.

```
RANDOM NUMBER [START:25000 END: 100000]
POST PROCESSING FUNCTION salary_post_processing
```

To create the `salary_post_processing` function, your code might look like the following:

```
CREATE OR REPLACE FUNCTION
salary_post_processing (rowid varchar2, column_name varchar2, mask_value
varchar2)
RETURN varchar2
IS
BEGIN
    RETURN ('$' || mask_value);
END;
```

Preserve Original Data

Purpose

The Preserve Original Data masking format retains the original values in a column. It is useful in conditional masking when you want to preserve a subset of values in a column and mask the remaining values using some other masking formats.

> **See Also:**
>
> Example 1: Protecting Sensitive Identifiers Across Diverse Geographic Regions

Inputs

- No inputs are required.

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: Yes
- Reversible: Does not apply
- Uniqueness: If the original values are unique, they will remain unique after masking.

Example

Assume that a table has a `SALARY` column that you want to mask by using the `EMPLOYEE ID` column in a condition. If the `EMPLOYEE ID` values are less than 100, you want to keep them. If they are from 100 to 199, you want to use the fixed number 100000. Any `EMPLOYEE ID` greater than or equal to 200, you want to use a random number between 30000 and 500000.

The masking logic for the SALARY column might look like the following:

```
EMPLOYEE_ID < 100
      PRESERVE ORIGINAL DATA
EMPLOYEE_ID < 200
      FIXED NUMBER 100000
EMPLOYEE_ID >= 200
      RANDOM NUMBER [Start Value: 30000 End Value: 500000]
```

Random Date

Purpose

The Random Date masking format generates random dates within a date range to replace the original column values.

Inputs

- **Start Date:** The lower bound of the range within which random dates should be generated
- **End Date:** The upper bound of the range within which random dates should be generated

The inputs should be in format YYYY-MM-DD. Start Date should be less than or equal to End Date.

Supported Data Types

- Character
- Date

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: Yes
- Deterministic: No
- Reversible: No
- Uniqueness: Yes. The total number of distinct values in the specified range must be greater than or equal to the number of values in the column.

Example

To generate random dates between January 1, 2016 and December 31, 2019 for the column BIRTH_DATE, you can use the Random Date masking format with the dates entered as the two parameters.

The following table shows the original BIRTH_DATE column and the MASKED_BIRTH_DATE column.

BIRTH_DATE	MASKED_BIRTH_DATE
01/01/2010	02/09/2016
05/02/2018	01/02/2018
09/11/2009	08/10/2019

Random Decimal Number

Purpose

The Random Decimal Number masking format generates random decimal numbers within a value range to replace the original column values.

Inputs

- **Start Number:** The lower bound of the range within which decimal numbers should be generated
- **End Number:** The upper bound of the range within which decimal numbers should be generated

The inputs can be any decimal numbers, including negative numbers. Start Number must be less than or equal to End Number. They should be valid for the column size.

Supported Data Types

- Character
- Numeric

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: Yes
- Deterministic: No
- Reversible: No
- Uniqueness: Yes. The total number of distinct values in the specified range must be greater than or equal to the number of values in the column.

Example

Suppose you have a `HEIGHT` column and you want to generate random heights from 0.5 through 2.2 meters. You can use the Random Decimals Number masking format to generate decimal numbers from 0.5 through 2.2, including those values.

Random Digits

Purpose

The Random Digits masking format generates random digits of length within a range. It pads to the appropriate length in a string, but does not pad when used for a number column. This format is a complementary type of Random Number, which is not padded.

Inputs

- **Start Length:** The minimum number of digits each masked value should have
- **End Length:** The maximum number of digits each masked value should have

Supported Data Types

- Character
- Numeric

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: Yes
- Deterministic: No
- Reversible: No
- Uniqueness: Yes, however, if you do not specify a sufficient length range, you can run out of unique values within the range.

Example

For a random digit with a length of [5,5], an integer from zero through 99999 is randomly generated and left padded with zeros to satisfy the length and uniqueness requirement.

Random List

Purpose

The Random List masking format randomly selects values from a list of values to replace the original column values.

Inputs

- **List of Values:** A comma-separated list of values that should be used to replace column values. The data type of each value in the list must be compatible with the data type of the column. If using a list of dates, the dates should be in format `YYYY-MM-DD`. The number of entries in the list cannot be more than 999.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: Yes
- Deterministic: No
- Reversible: No
- Uniqueness: Yes. The input list must have unique values, and the number of values in the list must be greater than or equal to the number of values in the column to be masked.

Example 1

Suppose you have a column with values 10, 20, 30, 40, 50. You can replace these values with random values from an input list (99, 100, 101, 102, 103) by using the Random List masking format. The following table compares the values in the original column (`ORIGINAL`) to the values after the first masking job (`MASK1`) and second masking job (`MASK2`). Notice that the masked values change each time the masking job runs.

ORIGINAL	MASK1	MASK2
10	101	100
20	103	99
30	100	101
40	99	102
50	102	103

Example 2

The following table shows you how a `MARITAL_STATUS` column, consisting of five distinct values, gets masked with the Random List masking format. The list of values for the masking format is Single, Married, and Divorced.

MARITAL_STATUS	MASKED_MARITAL_STATUS
Single	Divorced
Married	Single
Windowed	Divorced
Single	Married
Divorced	Married
Separated	Single

Random Number

Purpose

The Random Number masking format generates random integers within a specified range to replace column data.

Inputs

- **Start Number:** The lower bound of the range within which the integers should be generated.
- **End Number:** The upper bound of the range within which the integers should be generated.

The inputs can be any integers, including negative integers. Start Number must be less than or equal to End Number. They should be valid for the column size.

Supported Data Types

- Character
- Numeric

Characteristics

- Supports Double-Byte Characters: Does not apply
- Combinable: Yes
- Deterministic: No
- Reversible: No
- Uniqueness: Yes. The number of distinct values in the specified range must be greater than or equal to the number of values in the column.

Example

Suppose you have an `EMPLOYEE_AGE` column and you want to generate random ages from 21 through 65. You can use the Random Number masking format to generate random integers from 21 through 65, including those values.

The following table shows the original `EMPLOYEE_AGE` column and the `MASKED_EMPLOYEE_AGE` column.

EMPLOYEE_AGE	MASKED_EMPLOYEE_AGE
21	59
35	22
51	43
28	38
64	61
75	21

Random String

Purpose

The Random String masking format replaces column data with random strings of length within the specified range. The generated strings consist of lowercase letters only.

Inputs

- **Start Length:** The minimum number of characters that the generated strings should have.
- **End Length:** The maximum number of characters that the generated strings should have.

The inputs can be any integers greater than zero. Start Length must be less than or equal to End Length. The inputs should be valid for the column size.

Supported Data Types

- Character

Characteristics

- Supports Double-Byte Characters: No
- Combinable: Yes
- Deterministic: No

- Reversible: No
- Uniqueness: Yes. The number of distinct values in the specified range must be greater than or equal to the number of values in the column.

Example

Suppose you have a `FIRST_NAME` column and you want to mask it with random names of length from 5 through 15. You can use the Random String masking format to generate strings of desired length by entering these two values as input parameters.

Random Substitution

Purpose

The Random Substitution masking format enables you to mask values in a column using data from a substitution column. The values in the user-specified column are randomly ordered before mapping them to the original column values.

Inputs

- **Schema Name:** The name of the schema containing the substitution column
- **Table Name:** The name of the table containing the substitution column
- **Column Name:** The name of the substitution column containing the data that should be used for masking. The data types of the specified substitution column and column to be matched must be the same.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: No, because the Random Substitution masking format randomly orders the mask values in the substitution column before replacing the sensitive data (unlike the Deterministic Substitution masking format)
- Reversible: No
- Uniqueness: Yes. The number of distinct values in the substitution column must be greater than or equal to the number of values in the column to be masked.

Example

Suppose you discover a sensitive column named `EMP_ID` that contains employee IDs. Let's assume that you have fake employee ID values stored in another column named `SUB_EMP_ID`, which resides in the `SUB_EMPLOYEES` table in the `SUB_HR` schema (as shown in the following table).

SUB_EMP_ID
101
102
103
104
105
106
107

When configuring the masking policy in the Data Masking wizard, you can choose the Random Substitution masking format for the `EMP_ID` column. Provide the following inputs: `SUB_HR`, `SUB_EMPLOYEES`, and `SUB_EMP_ID`. When the job runs, Data Masking randomly orders the fake values in the `SUB_EMP_ID` column and uses them to replace the values in the `EMP_ID` column.

The following table compares the values in the original column (`EMP_ID`) to the values after the first masking job (`MASK1`) and second masking job (`MASK2`). Notice that the masked values change each time the masking job runs.

EMP_ID	MASK1	MASK2
412	101	104
185	107	105
102	105	102
322	102	101
692	103	106

Regular Expression

Purpose

The Regular Expression masking format gives you the flexibility to use regular expressions to search for sensitive data in a column of Character Large Object (CLOB) or National Character Large Object (NCLOB) data types, and replace the data with a fixed string, fixed number, or null value. You can also use this masking format for columns of `VARCHAR2` type to mask parts of strings.

Inputs

- **Regular Expression:** The pattern that should be used to search for sensitive data
- **Replace With:** The value that should be used to replace the data matching the regular expression

Supported Data Types

- Character
- Numeric
- Large Object (LOB) - CLOB and NCLOB only

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: No
- Reversible: No
- Uniqueness: No

Examples

- Use the regular expression `@abc\.com` to search for email addresses containing `@abc.com` and replace `@abc.com` with `@example.com`
- Use the regular expression `[A-Z]+@[A-Z]+\.[A-Z]{2,4}` to mask email addresses by replacing with `john.doe@abcd.com`
- Use the regular expression `[0-9]{3}[ -][0-9]{2}[ -][0-9]{4}` to match Social Security numbers and replace with `***-**-****`
- Use the regular expression `<SALARY>[0-9]{2,6}</SALARY>` to zero out salary information by replacing with `<SALARY>0</SALARY>`

Shuffle

Purpose

The Shuffle masking format randomly shuffles values within a column.

Shuffle preserves data distribution. Suppose a column has 100 values, and all values are either 21 or 10, and the value 21 appears 60 times and the value 10 appears 40 times, after shuffling this column, this count remains same.

Inputs

- No input values are required.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: No
- Reversible: No
- Uniqueness: Yes, provided the column values are all unique

Example

In the following table, the values in the SALARY column are shuffled in the SHUFFLED_SALARY column.

EMPLOYEE	JOB_CATEGORY	SALARY	SHUFFLED_SALARY
Alice	M	90	70
Bill	M	88	57
Carol	W	72	88
Denise	W	57	45
Eddie	W	70	90
Frank	W	45	72

SQL Expression

Purpose

The SQL Expression masking format lets you use a SQL expression to mask column data. Data Masking uses the specified SQL expression to generate values which are used to replace the original data.

Inputs

- **SQL Expression:** The SQL expression generates the masked values. It can consist of one or more values, operators, and SQL functions that evaluate to a value. It can also contain substitution columns (columns from the same table as the column to be masked). Specify the substitution columns within percent (%) symbols. Use SQL expressions with dbms_lob and other user-defined functions to mask columns of Large Object data type (LOBs include BLOB, CLOB, and NCLOB).

Supported Data Types

- Character
- Numeric
- Date
- Large Object (LOB)

Characteristics

- Supports Double-Byte Characters: Yes, the SQL expression provided should generate multi-byte characters
- Combinable: No
- Deterministic: Yes, depending on the SQL expression defined
- Reversible: No
- Uniqueness: Yes, but the uniqueness is not guaranteed and depends on the SQL expression defined. However, because ORA_HASH uses a 32-bit algorithm, and considering the birthday paradox or pigeonhole principle, there is a 0.5 probability of collision after 232-1 unique values.

Examples

- Generate random email addresses.

```
dbms_random.string('u', 8) || '@example.com'
```

- Generate email addresses using values from substitution columns, for example, `FIRST_NAME` and `LAST_NAME`.

```
%FIRST_NAME% || '.' || %LAST_NAME% || '@example.com'
```

- Empty a CLOB.

```
dbms_lob.empty_clob()
```

- Apply a custom masking function to a CLOB column, for example, `CLOB_COL`.

```
custom_mask_clob(%CLOB_COL%)
```

- Perform conditional masking. For example, the following expression masks `PERSON_FULL_NAME` with the first and last name if the party type is `PERSON`. Otherwise, it uses a random string to mask the data.

```
(case when %PARTY_TYPE%='PERSON' then %PERSON_FIRST_NAME%|| ' ' ||
%PERSON_LAST_NAME% else (select dbms_random.string('U', 10) from dual) end)
```

- Perform substitution masking. For example, the following expression selects 1000 rows in the substitution table, `DATA_MASK.DATA_MASK_ADDR`. It masks `%ZIPCODE%` with the `MASK_ZIPCODE` column in the substitution table. The row selected depends on `ora_hash` and is deterministic in this case. Selection is random if `dbms_random` procedures are used.

```
select MASK_ZIPCODE from DATA_MASK.DATA_MASK_ADDR where ADDR_SEQ =
ora_hash( %ZIPCODE% , 1000, 1234)
```

Substring

Purpose

The Substring masking format extracts a portion of the original column value, and uses that to replace the original value. This masking format is similar to the `SUBSTR` database function.

Inputs

- **Start Position:** The starting position in the original string from where the substring should be extracted. The start position can be either a positive or a negative integer. If the start position is negative, the counting starts from the end of the string.
- **Length:** The number of characters that you want in the substring. It should be an integer and greater than zero.

Supported Data Types

- Character

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: Yes
- Deterministic: Yes
- Reversible: No
- Uniqueness: No

Example

Suppose an original column value is `abcd`. A substring with a start position of 2 and length of 3 generates a masked string of `bcd`. A substring with start position of -2 and length of 3 generates a masked string of `cd`.

Truncate Data

Purpose

The Truncate Data masking format drops all the rows in a table. If one of the columns in a table is masked using Truncate Data, the entire table is truncated, so no other masking format can be used for any of the other columns in that table. If a table is being truncated, it cannot be referred to by a foreign key constraint or a dependent column.

Inputs

- No inputs are required.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: No
- Deterministic: Does not apply
- Reversible: Does not apply
- Uniqueness: Does not apply

Example

Suppose that you want to mask ten tables in a database schema. In one of the tables, all the columns contain highly sensitive data, and therefore, you do not want to share this table. You can use the Truncate Data masking format to drop all the rows in this table.

User Defined Function

Purpose

The User Defined Function masking format lets you define your own logic to mask column data. The return value of the user-defined function is used to replace the original values. The user-defined function is a PL/SQL function that can be invoked in a `SELECT` statement.

Inputs

- **Package Name:** The name of the database package
- **Function Name:** The name of the database function

The database function has a fixed signature:

```
function udf_func (rowid varchar2, column_name varchar2, original_value
varchar2) return varchar2;
```

where:

- `rowid` is the row identifier of the row containing the value to be masked.
- `column_name` is the name of the column to be masked.
- `original_value` is the column value to be masked.

Supported Data Types

- Character
- Numeric
- Date

Characteristics

- Supports Double-Byte Characters: Yes
- Combinable: Yes
- Deterministic: Yes, depending on the function defined
- Reversible: No
- Uniqueness: Yes, depending on the function defined

Example

Suppose you create a user-defined function to mask string values.

To create the user-defined function, you might use the following code to randomize the string values. This example is simple, however you can write more complex code to suit your business use case.

```
CREATE OR REPLACE FUNCTION
change_value (rowid varchar2, column_name varchar2, mask_value varchar2)
RETURN varchar2
IS
BEGIN
```

```
    RETURN DBMS_RANDOM.STRING('A',8);
END;
```

View Masking Formats

You can view Oracle predefined masking formats and user-defined masking formats from the Masking Formats page in Security Center. Becoming familiar with the predefined masking formats helps you to create masking policies.

Search for a Masking Format

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats**.

   The **Masking Formats** page is displayed.
3. Under **List Scope**, select the compartment that contains user-defined masking formats. No matter the compartment selected, all Oracle predefined masking formats are listed. Optionally select **Include child compartments** to also list user-defined masking formats in child compartments.
4. To filter the list of masking formats, do the following:
   a. (Optional) In the **Masking Format Name** field, enter the full and exact masking format name. The search is case-sensitive.
   b. (Optional) From the **Listing Type** drop-down list, select **All**, **Oracle Predefined**, or **User Defined** to show all masking formats, only Oracle predefined masking formats, or only user-defined masking formats, respectively.
   c. Click **Apply Filters**.
5. To browse pages, scroll to the bottom of the page and click the left and right arrow buttons.

View Details for a Masking Format

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats**.

   The **Masking Formats** page is displayed.
3. Search for and click the name of the masking format for which you want to view more information.

   The **Masking Format Details** page is displayed.
4. On the **Masking Format Information** tab, view the name of the masking format, description of the masking format, and whether the masking format is Oracle Predefined.
5. Under **Format Details**, view the format entries for the masking format, and the format entry details.

Create or Edit Masking Formats

You can create your own masking formats by using the basic masking formats in Oracle Data Safe as your starting point.

About Creating User-Defined Masking Formats

When creating user-defined masking formats, you select basic masking formats and then customize them to meet your specific requirements. The results of the masking formats are concatenated together. You can also choose to start with an existing masking format, edit it, and then save it under a different name.

You cannot apply conditions when creating a masking format. You can create conditions when you modify a masking format from within a masking policy.

Suppose you want to mask a national identifier that has ten digits. You can create a new masking format, say My National Identifier, using the Random Number masking format. Random Number takes two inputs: Start Number and End Number. You can provide 1000000000 as the Start Number and 9999999999 as the End Number, and then save your masking format. In the future, to mask a column containing that national identifier, you can simply choose the My National Identifier masking format. Input is not required. If you have a sensitive type to discover your national identifier, you can also set My National Identifier as the default masking format for that sensitive type. This way, whenever you discover columns using this sensitive type, Data Masking selects the mapped masking format by default.

Supported Data Types for User-Defined Masking Formats

Before creating a masking format for a sensitive column, first determine the column's data type. The data type dictates which basic masking formats you can use.

Character Data Types

The following character types can use Delete Rows, Deterministic Encryption, Deterministic Substitution, Fixed Number, Fixed String, Group Shuffle, Null Value, Post Processing Function, Preserve Original Data, Random Decimal Number, Random Digits, Random List, Random Number, Random String, Random Substitution, Regular Expression, Shuffle, SQL Expression, Substring, Truncate Data, and User Defined Function masking formats:

- `CHAR`
- `NCHAR`
- `VARCHAR2`
- `NVARCHAR2`

Numeric Data Types

The following numeric types can use Delete Rows, Deterministic Encryption, Deterministic Substitution, Fixed Number, Group Shuffle, Null Value, Post Processing Function, Preserve Original Data, Random Decimal Number, Random Digits, Random List, Random Number, Random Substitution, Regular Expression, Shuffle, SQL Expression, Truncate Data, and User Defined Function masking formats:

- `NUMBER`
- `FLOAT`
- `RAW`
- `BINARY_FLOAT`
- `BINARY_DOUBLE`

Date Data Types

The following date types can use Delete Rows, Deterministic Encryption, Deterministic Substitution, Group Shuffle, Null Value, Post Processing Function, Preserve Original Data, Random Date, Random List, Random Substitution, Shuffle, SQL Expression, Truncate Data, and User Defined Function masking formats:

- `DATE`
- `TIMESTAMP`

Large Object (LOB) Data Types

The following LOB data types can use Fixed Number, Fixed String, Null Value, Regular Expression, and SQL Expression masking formats:

- `BLOB`
- `CLOB`
- `NCLOB`

Unsupported Objects

Oracle Data Safe does not support masking for the following:

- External tables
- Clustered tables
- Queue tables
- Long columns
- XML-type columns
- Virtual columns
- `ROWID` columns
- JSON columns
- Graph tables

Create a User-Defined Masking Format

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats**.

   The **Masking Formats** page is displayed.
3. Click **Create Masking Format**.

   The **Create Masking Format** window is displayed.
4. Enter a name for your masking format.
5. Select a compartment in which to store your masking format.
6. (Optional) Enter a description for your masking format.
7. (Optional) If you want to create a masking format based on an existing masking format, do the following:

a. (Optional) If needed, click **Change Compartment**, and browse to and select the correct compartment. Oracle predefined masking formats are listed in all compartments. User-defined masking formats may reside in other compartments.

b. From the **Create Like Masking Format** drop-down list. Select an Oracle predefined masking format or a user-defined masking format. The masking format fields are automatically populated.

8. Configure the masking format.

   a. From the **Masking Format Entry** drop-down list, select a basic masking format and configure its parameters. Or, if you previously selected a masking format to copy, edit the existing parameters as needed.

   b. To add another masking format, click **Add Format Entry** and configure its parameters. If you enter more than one masking format, the masking formats will be concatenated.

   c. To delete a masking format, click the **X** button next to it.

9. Click **Create Masking Format**.

   Your new masking format is now displayed on the **Masking Formats** page. You can select your masking format whenever you create a data masking job.

Edit a User-Defined Masking Format

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats**.

   The **Masking Formats** page is displayed.
3. Search for and click the name of your masking format.

   The **Masking Format Details** page is displayed.
4. Click **Edit**.

   The **Edit Masking Format** window is displayed.
5. (Optional) Modify the name and/or description of the masking format.
6. (Optional) Modify existing masking format entries.
7. (Optional) To add another masking format entry, click **+ Another Format Entry**, select a basic masking format, and then configure its values.
8. (Optional) To delete a masking format, click the **X** button next to the right of the masking format entry.
9. Click **Save**.

   The masking format is immediately updated.

Create Masking Policies

You can create a masking policy from a sensitive data model or create an empty masking policy for a target database and add columns later.

About Creating Masking Policies

You can create masking policies from the **Masking Policies** page in Oracle Data Safe. You have a two options when creating a masking policy:

- Create a masking policy starting with a sensitive data model. To use this option, you need to have access to a pre-built sensitive data model. Oracle Data Safe lists all the sensitive columns from the sensitive data model and automatically associates them with default masking format. You can then modify and edit the selections as needed.
- Create an empty masking policy and associate it with a target database. Later, you add columns to the masking policy and associate masking formats with them.

Create a Masking Policy Starting From a Sensitive Data Model

Create a masking policy starting from data masking

1. Under **Security center**, click **Data masking**.
2. Under **Related resources**, click **Masking policies**. The **Masking policies** page is displayed.
3. Click **Create masking policy**. The **Create masking policy** window is displayed.
4. Enter a name for your masking policy.
5. Select a compartment in which to store your masking policy.
6. (Optional) Enter a brief description of your masking policy.
7. Leave the **Using a sensitive data model** tile selected.
8. Select a sensitive data model. If needed, click **Change compartment**, and browse to and select a different compartment.
9. (Optional) To upload pre-masking and post-masking scripts, do the following:
   a. Expand **Upload Scripts**.
   b. In the **Upload Pre-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.
   c. In the **Upload Post-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.

   Limitations and usage notes of using pre-masking or post-masking scripts:
   - SQL statements and PL/SQL blocks are executed sequentially from the provided pre or post masking scripts.
   - When processing the scripts, Data Safe is capable of creating and executing all PL/SQL stored program units (procedures, functions, packages, anonymous block).
   - If execution of any statement or block fails, the errors and warnings are ignored and execution of subsequent statements is continued.
   - Data Safe automatically retries the script execution, up to seven times, from the beginning if interrupted due to database connectivity issues. Therefore, we recommend ensuring that pre and post masking scripts can be run repetitively without impacting the results.
   - Along with successfully executed statements, errors of failed statements can be viewed in the downloadable masking log file.

Failed statements and the errors are also available as part of work-request errors which can be viewed on the Data Safe console.

- Data Safe does not support printing the output of `DBMS_OUTPUT.PUT_LINE()` statements to the downloadable masking log file.
- Data Safe does not support printing the output of any third-party PL/SQL logging libraries to the downloadable masking log file.
  The output of `SELECT` queries is also not printed in the downloadable masking log file. The workaround for this is to write the output of `SELECT` queries to a table which could be queried later.
- Data Safe does not support execution of another SQL script file from the pre or post masking scripts.
- Data Safe does not support functionality specific to the SQL*Plus client.

10. (Optional) To customize the processing of the masking job, do the following:
    a. Expand **Masking Options**
    b. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.
    c. Specify the value for parallel execution:
       - **NONE** - No parallelism is used when data masking process is running.
       - **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
       - **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

       > **Note:**
       >
       > The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

    d. Specify how you would like invalid objects to recompile after data masking:
       - **NONE** - Invalid objects do not recompile.
       - **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.
       - **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

       > **Note:**
       >
       > If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

    e. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary

tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

> **Note:**
>
> Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

f. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

11. (Optional) To create tags, click **Show Advanced Options** and configure tags for your masking policy.
12. Click **Create masking policy**.

> **Note:**
>
> It's important that you wait for the masking policy to be created before closing the window so that all sensitive columns from the sensitive data model are successfully added to the masking policy. When the masking policy is fully created, the **Masking Policy Details** page is displayed and the status is set to **ACTIVE**.

13. Review your masking policy.
    - The **Masking Policy Information** tab shows you the name and OCID of your masking policy, the work request information, the compartment in which the masking policy is stored, the target database with which the masking policy is associated, the name of the sensitive data model, and when the masking policy was created and last updated.
    - The **Masking Columns** section shows you the list of sensitive columns, their associated default masking formats, and if they have associated child columns.

Create masking policy from Sensitive data model details

1. Under **Security center**, click **Data discovery**.
2. Under **Related resources**, click **Sensitive data models**. The **Sensitive data models** page is displayed.
3. Click on the name of a specific Sensitive Data Model. The **Sensitive data model details** page is displayed.
4. Click **Create masking policy**. The **Create masking policy** window is displayed.
5. Enter a name for your masking policy.
6. Select a compartment in which to store your masking policy.
7. (Optional) Enter a brief description of your masking policy.
8. Leave the **Sensitive data model** as listed.
9. (Optional) To upload pre-masking and post-masking scripts, do the following:
   a. Expand **Upload Scripts**.
   b. In the **Upload Pre-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.

c. In the **Upload Post-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.

Limitations and usage notes of using pre-masking or post-masking scripts:

- SQL statements and PL/SQL blocks are executed sequentially from the provided pre or post masking scripts.
- When processing the scripts, Data Safe is capable of creating and executing all PL/SQL stored program units (procedures, functions, packages, anonymous block).
- If execution of any statement or block fails, the errors and warnings are ignored and execution of subsequent statements is continued.
- Data Safe automatically retries the script execution, up to seven times, from the beginning if interrupted due to database connectivity issues. Therefore, we recommend ensuring that pre and post masking scripts can be run repetitively without impacting the results.
- Along with successfully executed statements, errors of failed statements can be viewed in the downloadable masking log file.
  Failed statements and the errors are also available as part of work-request errors which can be viewed on the Data Safe console.
- Data Safe does not support printing the output of `DBMS_OUTPUT.PUT_LINE()` statements to the downloadable masking log file.
- Data Safe does not support printing the output of any third-party PL/SQL logging libraries to the downloadable masking log file.
  The output of `SELECT` queries is also not printed in the downloadable masking log file. The workaround for this is to write the output of `SELECT` queries to a table which could be queried later.
- Data Safe does not support execution of another SQL script file from the pre or post masking scripts.
- Data Safe does not support functionality specific to the SQL*Plus client.

10. (Optional) To customize the processing of the masking job, do the following:
    a. Expand **Masking Options**
    b. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.
    c. Specify the value for parallel execution:
       - **NONE** - No parallelism is used when data masking process is running.
       - **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
       - **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

> **Note:**
>
> The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

d. Specify how you would like invalid objects to recompile after data masking:
   - **NONE** - Invalid objects do not recompile.
   - **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.
   - **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

   > **Note:**
   >
   > If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

e. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

   > **Note:**
   >
   > Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

f. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

11. (Optional) To create tags, click **Show advanced options** and configure tags for your masking policy.
12. Click **Create masking policy**.

    > **Note:**
    >
    > It's important that you wait for the masking policy to be created before closing the window so that all sensitive columns from the sensitive data model are successfully added to the masking policy. When the masking policy is fully created, the **Masking Policy Details** page is displayed and the status is set to **ACTIVE**.

13. Review your masking policy.
    - The **Masking Policy Information** tab shows you the name and OCID of your masking policy, the work request information, the compartment in which the masking policy is stored, the target database with which the masking policy is associated, the name of the sensitive data model, and when the masking policy was created and last updated.
    - The **Masking Columns** section shows you the list of sensitive columns, their associated default masking formats, and if they have associated child columns.

Create an Empty Masking Policy and Associate it With a Target Database

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**. The **Masking Policies** page is displayed.
3. Click **Create Masking Policy**. The **Create Masking Policy** window is displayed.
4. Enter a name for your masking policy.
5. Select a compartment in which to store your masking policy.
6. (Optional) Enter a brief description of your masking policy.
7. Select the **Using a target database** tile.
8. Select a target database. If needed, click **Change Compartment**, and browse to and select a different compartment.
9. (Optional) To upload pre-masking and post-masking scripts, do the following:
   a. Expand **Upload Scripts**.
   b. In the **Upload Pre-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.
   c. In the **Upload Post-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.

   Limitations and usage notes of using pre-masking or post-masking scripts:

   - SQL statements and PL/SQL blocks are executed sequentially from the provided pre or post masking scripts.
   - When processing the scripts, Data Safe is capable of creating and executing all PL/SQL stored program units (procedures, functions, packages, anonymous block).
   - If execution of any statement or block fails, the errors and warnings are ignored and execution of subsequent statements is continued.
   - Data Safe automatically retries the script execution, up to seven times, from the beginning if interrupted due to database connectivity issues. Therefore, we recommend ensuring that pre and post masking scripts can be run repetitively without impacting the results.
   - Along with successfully executed statements, errors of failed statements can be viewed in the downloadable masking log file.
     Failed statements and the errors are also available as part of work-request errors which can be viewed on the Data Safe console.
   - Data Safe does not support printing the output of `DBMS_OUTPUT.PUT_LINE()` statements to the downloadable masking log file.
   - Data Safe does not support printing the output of any third-party PL/SQL logging libraries to the downloadable masking log file.
     The output of `SELECT` queries is also not printed in the downloadable masking log file. The workaround for this is to write the output of `SELECT` queries to a table which could be queried later.
   - Data Safe does not support execution of another SQL script file from the pre or post masking scripts.
   - Data Safe does not support functionality specific to the SQL*Plus client.
10. (Optional) To customize the processing of the masking job, do the following:
    a. Expand **Masking Options**

b. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.

c. Specify the value for parallel execution:

- **NONE** - No parallelism is used when data masking process is running.
- **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
- **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

> **Note:**
>
> The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

d. Specify how you would like invalid objects to recompile after data masking:

- **NONE** - Invalid objects do not recompile.
- **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.
- **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

> **Note:**
>
> If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

e. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

> **Note:**
>
> Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

f. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

11. (Optional) To create tags, click **Show Advanced Options** and configure tags for your masking policy.
12. Click **Create Masking Policy**. The **Masking Policy Details** page is displayed. When the masking policy is successfully created, the status is set to **ACTIVE**.
13. Review your empty masking policy.

- The **Masking Policy Information** tab shows you the name and OCID of your masking policy, the work request information, the compartment in which the masking policy is stored, the target database with which the masking policy is associated, and when the masking policy was created and last updated.
- The **Masking Columns** section is empty. You can add and remove columns as needed.

View Masking Policies

You can view masking policies from the **Masking Policies** page. Masking policies are either created from this page or uploaded to this page.

Search for a Masking Policy

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Under **List Scope**, select the compartment that contains your masking policy. Optionally select **Include child compartments** to include masking policies in the list from child compartments.
4. To filter the list of masking policies, under **Filters**, do the following:
   a. (Optional) To search by state: From the **State** drop-down list, select a state (**Any state**, **Creating**, **Updating**, **Active**, **Deleting**, **Deleted**, or **Failed**).
   b. (Optional) Select a target database from the **Target database** menu.
   c. (Optional) To search by name: In the **Masking Policy Name** box, enter the full and exact masking policy name. The search is case-sensitive.
   d. (Optional) Select time created before from the **Time created before** menu.
   e. Click **Apply Filters**.
5. (Optional) If there are multiple pages of masking policies, click the left and right navigation arrow buttons at the bottom of the page to navigate between pages.

View Details for a Masking Policy

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Search for and click the name of the masking policy that you want to view.

   The **Masking Policies Details** page is displayed.
4. View the masking policy details.
   - The **Masking Policy Information** tab shows you the name and Oracle Cloud Identifier (OCID) of your masking policy, the work request information, the compartment in which the masking policy is stored, the target database with which the masking policy is associated, the name of the sensitive data model, and when the masking policy was created and last updated.
   - The **Masking Columns** section shows you the list of sensitive columns, their associated masking formats, and if a column has child columns.

- If a column has child columns, click on **View Details** to view the name and location of the child column(s).

> **Note:**
>
> Child column(s) will have the same masking format applied as their parent columns.

5. To view the work requests related to the masking policy, you can do the following:
   a. To view the latest work request, on the **Masking Policy Information** tab, click the **View Details** link next to **Work Request**. The **Work Request** page is displayed. Here you can view the work request information, log messages, and error messages (select **Error Messages** under **Resources**).
   b. To view all the work requests for the past seven days (work requests are stored for only 7 days in Oracle Cloud Infrastructure), under **Resources**, click **Work Requests**. From here, you can view the status (for example, SUCCEEDED or FAILED), percent completed, date started, and date finished details for each work request. Click a particular work request to view its log messages and error messages.
   c. (Optional) If there was a work request failure, notice the error message displayed at the top of the page, for example, "There is at least one work request associated with this policy that has failed."
6. To explore the list of masking columns, do the following:
   a. Select one or more schemas from the **Schema name** list. Click **Load more** if there are more than 1000 schemas and your desired schema is not already listed.
   b. Select one or more tables from the **Table name** list. Click **Load more** if there are more than 1000 tables and your desired table is not already listed.
   c. Select one or more columns from the **Column name** list. A list of columns will only be available once either a schema or table is selected. Click **Load more** if there are more than 1000 columns and your desired column is not already listed.
   d. Click **Show More Options** to filter by sensitive type.
   e. Select a sensitive types from the **Sensitive Type** list. Click **Load more** if there are more than 1000 sensitive types and your sensitive type is not already listed.
   f. When all of your filters are created, click **Apply**.
   g. To remove a filter, click the **X** button next to the selected item.
7. To view referential relationships, under **Resources**, click on **Referential relationships**.

Edit Masking Policies

After you generate the initial masking policy for a target database, you most likely will need to edit it. For example, you might need to address sensitive columns that do not have an associated masking format, change masking formats, apply conditions to some masking formats, mask related columns together as a group (group masking), or add or remove columns from the masking policy.

Fix Columns that Need Attention

If you have one or more columns in your masking policy that are not automatically associated with a masking format, you need to address these columns. This may happen in the following scenarios:

- The sensitive column was discovered by a user-defined sensitive type, but the sensitive type does not have a default masking format assigned to it.
- Data Safe tried to associate a masking format, but it was not possible. This could've happened in the following scenarios:
  - The column contains a value that is incompatible with the column format
  - The assigned masking format generates data that exceeds the column size
  - The masking format does not guarantee sufficient number of distinct values which could lead to loss of data integrity

You can quickly find the list of columns needing your attention on the **Masking Columns Needing Attention** page.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of your masking policy to view its details.
4. Under **Resources**, click **Masking Columns Needing Attention**.
5. Locate the rows that have an exclamation mark next to the masking policy. Hover your mouse over the exclamation mark to learn about the issue.
6. Select a different masking format for the rows or edit the existing masking formats to resolve the issues. When a masking format is successfully updated, a message states **Masking Format Updated Successfully**.

Change or Edit the Masking Format for a Sensitive Column

By default, Oracle Data Safe associates a masking format with each sensitive column in a masking policy. If needed, you can select a different masking format or edit the default masking format.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of your masking policy to view its details.
4. Scroll down to the **Masking Columns** section where all the columns are listed with their associated masking formats.
5. Locate the row for the column for which you want to change the masking format.

> **Note:**
>
> You can't change the masking format of a column that is part of a composite relationship. The default masking format will be created following a naming convention of `schema.parenttable.datetime`. This `schema.parenttable.datetime` masking format will automatically apply group masking with shuffle format when a masking job is initiated. See Add or Remove a Referential Relationship from a Sensitive Data Model and Group Masking Example Using Shuffle for more information.

6. Perform one of the following actions to change the masking format:
   - From the **Masking Format** drop-down list, select a different predefined masking format. The **Edit Masking Format** page is displayed with the new masking format configuration. Edit the values as needed, and then click **Continue**.
   - Click the pencil button next to the masking format to open the **Edit Masking Format** page. Select a different masking format, configure the parameters, and then click **Continue**.
7. (Optional) Repeat step 6 to change the masking formats of other columns.
8. Verify that the highlighted rows are the ones that contain the masking format updates that you want. Note that your updates are not yet saved. If you navigate away from this page without saving, your changes will be lost.
9. To save all masking format updates at one time, click **Save Masking Formats**.

Add Columns to a Masking Policy

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of your masking policy to view its details.
4. Scroll down to the **Masking Columns** section and click **Add Columns**.

   The **Add Columns** window is displayed.
5. (Optional) If the schemas on the target database have been updated since the stated time and date, click **Refresh Database Schemas**.
6. Select the sensitive type that best describes the columns that you want to add to your masking policy.
7. Find columns by entering or selecting one or more of the following items, and then click **Search**.
   - **Schema name**
   - **Table name**
   - **Column name**

   A list of columns that match your selection criteria are displayed.
8. (Optional) Change the sensitive type of a column by selecting a new sensitive type from the **Sensitive Type** column.
9. Select the columns that you want to add to your masking policy, and then click **Add Columns**. To select all the columns, select the check box next to the **Schema** column heading.

The columns are added to the masking policy.

Add Previously Removed Columns to a Masking Policy

You can view the list of columns that were removed from a masking policy in the past and add them back to the masking policy if needed.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.

   A list of masking policies to which you have access is displayed.
3. Click the name of the masking policy for which you want to view or add previously removed columns.
4. Scroll down to the **Masking Columns** list and click **View/Add Previously Removed Columns**.

   The **Add Previously Removed Columns** panel shows the schema, table, column, and data type for each previously removed column.
5. To add all previously removed columns back to the masking policy, select **All columns**.
6. To add specific columns back to the masking policy, select **Select specific columns**, and then select individual columns from the list.
7. Click **Add Columns to Masking Policy**.

Remove Columns from a Masking Policy

You can remove columns from your masking policy that you don't want to mask on the target database. Note that the underlying sensitive data model is not affected.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of your masking policy to view its details.
4. Scroll down to the **Masking Columns** section where all the columns are listed with their associated masking formats.
5. To remove a singular column, click the symbol to the right of **Masking Column** to be removed in the **Masking Columns** list.
   a. Click the **Remove** option.
   b. Click **Remove Column** in the dialog box to confirm the removal of the column.
6. To remove multiple columns, click **Remove Columns** above the **Masking Columns** list. The **Remove Columns** window is displayed.
   a. (Optional) Select a sensitive type that best describes the columns that you want to remove.
   b. Enter or select one or more of the following items, and then click **Search**.
      - **Schema name**
      - **Table name**
      - **Column name**

      A list of sensitive columns that match your selection criteria are displayed.

c. Select the columns that you want to remove from your masking policy, and then click **Remove Columns**.

   To select all the columns, select the check box next to the **Schema** column heading. The columns are removed from the masking policy and the masking policy is automatically saved.

Update Tags, Masking Scripts, and Masking Options for a Masking Policy

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**
3. Click the name of your masking policy to view its details
4. From the **More Actions** menu select either **Add Tags**, **Update Pre/Post Masking Scripts**, or **Update Masking Options**.
5. (Optional) If you would like to add or update tags for your masking policy, configure them in the pop-up after selecting **Add Tags**. Select the **Tag Namespace**, **Tag Key**, and **Tag Value** from the drop-down lists.
6. (Optional) To upload pre-masking and post-masking scripts, do the following after selecting **Update Pre/Post Masking Scripts**:
   a. In the **Upload Pre-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.
   b. In the **Upload Post-Masking Script** area, drop your SQL file. Or, click the select one link, browse to and select your SQL file, and click **Open**.
7. (Optional) To customize the execution of the Masking Policy, do the following after selecting **Update Masking Options**:
   a. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.
   b. Specify the value for parallel execution:
      - **NONE** - No parallelism is used when data masking process is running.
      - **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
      - **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

      > **Note:**
      >
      > The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

   c. Specify how you would like invalid objects to recompile after data masking:
      - **NONE** - Invalid objects do not recompile.
      - **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.

- **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

> **Note:**
>
> If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

d. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

> **Note:**
>
> Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

e. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

Compare a Masking Policy to a Sensitive Data Model

When a sensitive data model is modified, a comparison to an associated masking policy can be initiated. The comparison identifies any differences between the sensitive data model and masking policy and allows you to select changes that will sync with the masking policy.

To run a comparison between a masking policy and it's associated sensitive data model:

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Select a masking policy from the list.
4. Under **Resources**, click **Compare with Sensitive Data Model**.
   This is only available if the masking policy is associated with a sensitive data model.
5. Click the **Compare with Sensitive Data Model** button.
6. Click **Submit**.
7. Once the comparison is complete, review any changes and select any changes that you like to sync under **Planned Actions**.
8. If you did not select all the changes in the previous step, click the **Save Changes for Planned Actions** button.
   a. Click **Save**.
9. Click the **Synchronize Masking Policy** button.
10. Click the **Synchronize Masking Policy** button in the confirmation dialog.

Once complete the masking policy will be updated with all changes that were selected.

Conditional Masking

Conditional masking allows you to set multiple logical conditions that alter the masking format of a masking column. Conditional masking can only be done when editing an existing masking format of a masking column in a masking policy.

Example 1: Protecting Sensitive Identifiers Across Diverse Geographic Regions

Learn how conditional masking can be used to mask unique personal identifiers based on country.

Problem

A large organization manages a database containing personal identifiers such as Social Security Numbers, National Insurance Numbers, and so on from individuals living in various countries. They are required by regulations and data protection laws to safeguard the sensitive information while having to maintain usability for authorized purposed. However, sharing this data for testing, development, or analysis poses significant privacy risks.

Solution

By utilizing Data Masking available in Data Safe, the organization is able to assign the appropriate masking formats to the personal identifiers to meet the privacy regulations. Using conditional masking allows for the masking format to change based on the country of residence listed in the database.

Consider the database contains the following information:

Table 7-1 Employee Personal Identifiers, Pre-Masking

Employee	Country	Identifier
Alice	US	987-65-4320
Bill	UK	BH 123654G
Carol	UK	AJ 763482K
Denise	US	798-66-4329

Following the implementation of a conditional masking format conditional on the country, the database may look something like the following:

Table 7-2 Employee Personal Identifiers, Post-Masking

Employee	Country	Identifier
Alice	US	674-58-2371
Bill	UK	PA 123456C
Carol	UK	AB 987654B
Denise	US	543-23-5431

Benefits

By implementing conditional masking formats, an organization:

- Prevents unauthorized access to sensitive personal identifiers.
- Complies with diverse regional privacy laws and data protection requirements.
- Preserves data integrity and usefulness for authorized activities, such as testing and analysis.
- Reduces the risk of data breaches and potential harm to individuals.
- Enables secure data sharing for collaboration and knowledge advancement.

Related Topics

- Add Conditions to a Masking Format
  See the steps and examples below to implement conditional masking formats in your masking policies.

Example 2: Protecting Sensitive Salary Data Across Different Employee Groups

Learn how conditional masking can be used to mask salary data based on an employee's role.

Problem

A company needs to analyze salary data to identify potential pay gaps between different employee groups, but is unable to share actual salary figures due to internal privacy concerns or competitive reasons.

Solution

By utilizing Data Masking available in Data Safe, the company is able to create a pseudonymized dataset suitable for salary disparity analysis. Using conditional masking allows for the original salary data to be masked by a random number in a specified range based on the employee group.

Consider the database contains the following information:

Table 7-3 Employee Salary Data, Pre-Masking

Employee	Job Category	Salary
Alice	Manager	90,000
Bill	Manager	88,000
Carol	Worker	72,000
Denise	Worker	57,000
Eddie	Worker	70,000
Frank	Worker	45,000
George	Assistant	45,000

Following the implementation of a conditional masking format conditional on the following:

- If job category is Manager, replace salary with a random number from 100000 through 150000.

- If job category is Worker, set salary to a fixed number (75000).
- Default is to preserve the existing value.

The database may look something like the following:

Table 7-4 Employee Salary Data, Post-Masking

Employee	Job Category	Salary
Alice	Manager	100,200
Bill	Manager	132,000
Carol	Worker	75,000
Denise	Worker	75,000
Eddie	Worker	75,000
Frank	Worker	75,000
George	Assistant	45,000

Benefits

By implementing conditional masking formats, the company:

- Protects individual employee salary information while enabling analysis of potential pay gaps between different job categories.
- Maintains data utility by creating a masked dataset that retains the statistical properties necessary for identifying salary disparity trends.
- Supports internal fairness by enabling data-driven decisions to promote fair compensation practices within the organization.

Related Topics

- Add Conditions to a Masking Format
  See the steps and examples below to implement conditional masking formats in your masking policies.

Add Conditions to a Masking Format

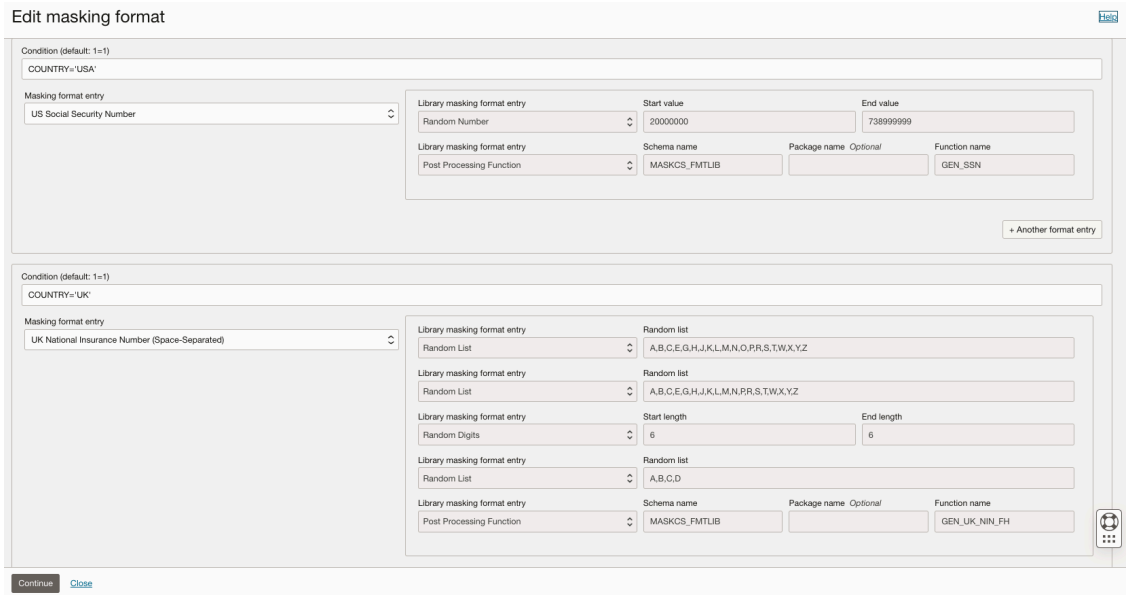
See the steps and examples below to implement conditional masking formats in your masking policies.

1. Under **Security center**, click **Data masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of a masking policy.
4. Locate the row for the column for which you want to add conditional masking in the Masking Columns section.
5. Click the pencil icon to edit the masking format.
6. Enter the desired condition in the **Condition** field, removing the default condition 1=1.
7. Select the **Masking Format Entry**.
8. Fill out any additional fields related to the selected masking format.
9. To add another condition, click **Another Masking Format** and repeat steps six through eight.

10. Click **Continue** once you have set all your conditional masking formats.

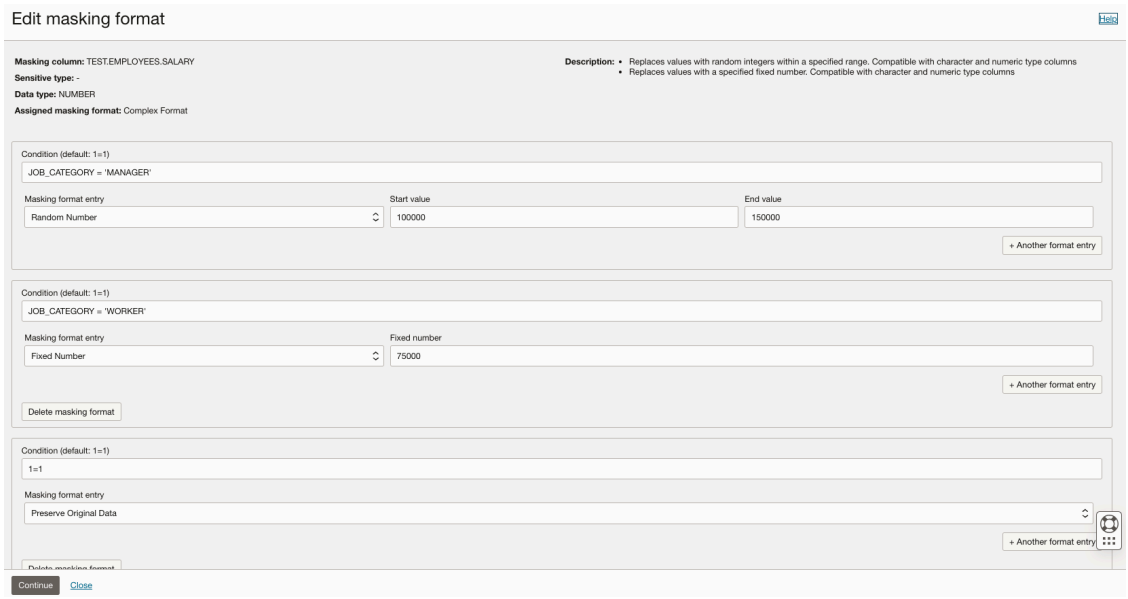
Example 7-1 Personal Identifiers Based on Country

In this example the goal is to create a masking format where unique personal identifiers are masked differently based on the country that the unique personal identifiers apply to. American (USA) identifiers can be masked using the Social Security Number masking format, and British (UK) identifiers can be masked using the National Insurance Number masking format. The below screenshot shows the conditions that could be set to implement a similar conditional masking format.



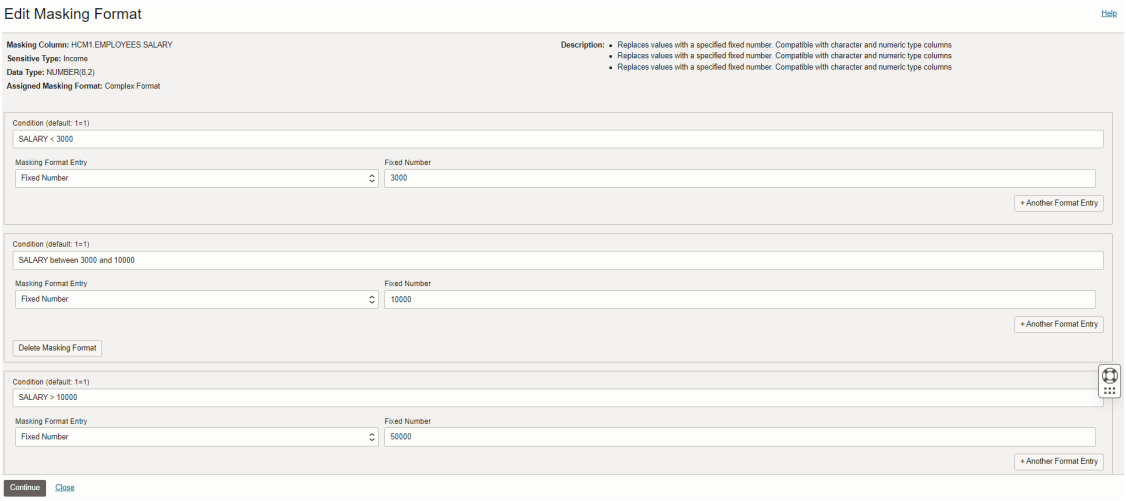
Example 7-2 Fixed Salary Based on Job Category

In this example the goal is to create a masking format where salaries are masked by being set to different values based on the employees job category. The below screenshot shows the conditions that could be set to implement a similar conditional masking format.



Example 7-3 Fixed Salary Based on Salary Amount

In this example the goal is to create a masking format where salaries are masked by being set to fixed values based on the salary amount. The below screenshot shows the conditions that could be set to implement a similar conditional masking format.



Related Topics

- Conditional Masking
  Conditional masking allows you to set multiple logical conditions that alter the masking format of a masking column. Conditional masking can only be done when editing an existing masking format of a masking column in a masking policy.

Group Masking

Group masking, also known as compound masking, enables you to mask related columns together as a group, ensuring that the masked data across the related columns retain the same relationship. You can use the group masking feature when you create data masking jobs.

About Group Masking

In a masking policy, the columns being masked as a group must belong to the same table. You can use the Shuffle, User Defined Function, Deterministic Substitution, and Random Substitution masking formats for group masking. The Deterministic Substitution and Random Substitution masking formats use data from another table to mask your sensitive data.

Group Masking Example Using Shuffle

The following is an example of group masking using the Shuffle masking format. Suppose that you have customers from across the world. You have their details stored in a table, as shown below.

CUST_ID	CUST_NAME	CITY	STATE	COUNTRY
678123	Michael Lee	Denpasar	Bali	Indonesia
678124	Sophia Lopes	Rio de Janeiro	Rio de Janeiro	Brazil
678125	Richard Williams	Santa Clara	California	United States
678126	Aaryan	Mumbai	Maharashtra	India

You don't want your developers to know the location of your customers. So, you want to mask the `CITY`, `STATE` and `COUNTRY` columns before sharing this data with the development team. But you want to have realistic masked data. For example, Richard lives in Santa Clara, California in the United States. After masking, if the city and state are Atlanta and Georgia respectively, India as the country is not valid. In this case, you want to ensure that the country remains the United States.

You can group these columns and use the Shuffle masking format to shuffle them together. After shuffling, your masked data might look like the data shown below.

CUST_ID	CUST_NAME	CITY	STATE	COUNTRY
678123	Michael Lee	Mumbai	Maharashtra	India
678124	Sophia Lopes	Denpasar	Bali	Indonesia
678125	Richard Williams	Rio de Janeiro	Rio de Janeiro	Brazil
678126	Aaryan	Santa Clara	California	United States

Group Masking Example Using Deterministic Substitution

This example shows you how to use the Deterministic Substitution masking format with group masking to mask sensitive data with data from another table. Suppose that you have customers from across the world. You have their details stored in a table, as shown below.

CUST_ID	CUST_NAME	CITY	STATE	COUNTRY
678123	Michael Lee	Denpasar	Bali	Indonesia
678124	Sophia Lopes	Rio de Janeiro	Rio de Janeiro	Brazil
678125	Richard Williams	Santa Clara	California	United States
678126	Aaryan	Mumbai	Maharashtra	India

Let's assume that you want to use the data from the following table for group masking:

SUB_CITY	SUB_STATE	SUB_COUNTRY
New York	New York	United States
Noida	Uttar Pradesh	India
Toronto	Ontario	Canada
Cape Town	Western Cape	South Africa

After masking these columns using the group masking option with the Deterministic Substitution masking format, your masked data might look like the data shown below.

CUST_ID	CUST_NAME	CITY	STATE	COUNTRY
678123	Michael Lee	Cape Town	Western Cape	South Africa

CUST_ID	CUST_NAME	CITY	STATE	COUNTRY
678124	Sophia Lopes	Toronto	Ontario	Canada
678125	Richard Williams	New York	New York	United States
678126	Aaryan	Noida	Uttar Pradesh	India

Mask Related Columns Together as a Group (Group Masking)

You can mask related columns together as a group, ensuring that the masked data across the related columns retain the same relationship.

1. Open a masking policy and scroll down to the **Masking Columns** section.
2. Select **Group Masking** from the drop-down list for one of the columns that is part of the group.

   The **Edit Masking Format** page displayed. By default, the **Group Name** field, **Masking Format Entry** drop-down list, and the column are displayed. You can add and remove columns from the group.
3. In the **Group Name** field, enter a new group name if this is the beginning of a group masking configuration. Or, select an existing group name if you want to add the column to an existing group masking configuration.
4. From the **Masking Format Entry** drop-down list, select the masking format that you want to apply to the columns in the group. You can select **Shuffle**, **Deterministic Substitution**, **Random Substitution**, or **User Defined Function**.
5. If you selected **Shuffle** as the masking format in step 4, you can optionally enter "group by" column names in the **Group Columns** box.
6. If you selected **Deterministic Substitution** as the masking format in step 4, enter the name of the substitution schema and table. Also, for each column listed, enter the name of the substitution column.
7. If you selected **Random Substitution** as the masking format in step 4, enter the name of the substitution schema and table. Also, for each column listed, enter the name of the substitution column.
8. If you selected **User Defined Function** as the masking format in step 4, enter the name of the schema and function for each column listed. Optionally, you can also enter a package name.
9. To add another column to the group, click **Add Column**.

   You can repeat this step until all columns in the table are listed, after which point the **Add Column** button becomes unavailable. Make sure that the column you initially selected to configure in step 2 is listed.
10. To remove a column from the group, select the check box for the column, and then click **Remove Column**.
11. Click **Save**.

Pre-Masking Check

Prior to initiating a masking job, a pre-masking check must be run. The pre-masking check performs a number of checks on the selected target database to determine if it is properly configured for a masking job.

The pre-masking check performs the following checks:

Table 7-5 Pre-masking checks

Check	Description
Database target user has been granted all required privileges	Check if the Data Safe service account on the target database has sufficient privileges to perform masking. For more information see, Grant Roles to the Oracle Data Safe Service Account on Your Target Database.
Maximum space required 65536 bytes. Tablespace DATA and the TEMP tablespace have the required free space	Check whether the user's default tablespace and TEMP tablespace have sufficient free space for masking. Masking requires the TEMP tablespace to be at least twice the size of the largest table being masked, and the default tablespace to be at least three times its size. For more information see, Create an Oracle Data Safe Service Account on a Target Database.
No invalid objects found	Check if there are invalid dependent objects of the tables being masked. Masking involves dropping and recreating the existing tables being masked and their dependent objects. Masking might run into issues recreating the invalid objects.
Database/system level triggers	Check if there are database/system-level triggers. Masking involves dropping and recreating the existing tables being masked and their dependent objects, such as triggers. Masking users may not have the privileges to drop database/system-level triggers, so masking might run into errors.
Tables in the masking policy have statistics up-to-date	Check if the tables being masked have up-to date statistics. Current statistics allow precise computation of space usage and other operations which rely on dictionary statistics. For more information see, GATHER_TABLE_STATS Procedure in the *Oracle Database PL/SQL Packages and Types Reference* guide.
Tables in the masking policy have no Oracle Label Security (OLS) policies	Check if the tables being masked have Oracle Label Security (OLS) policies applied. In order for the masking job to run properly, OLS policies affecting the table need to be dropped or disabled. **Post-masking, you will need to rebuild the OLS policies.** For more information on OLS, see the *Oracle Label Security Administrator's Guide*.

Table 7-5 (Cont.) Pre-masking checks

Check	Description
Virtual Private Database (VPD): The Data Safe user has access or VPD policies are disabled on the tables in the masking policy	Check if the tables being masked have Virtual Private Database (VPD) policies applied. In order for the masking job to run properly, the Data Safe user must be granted sufficient privileges to access the table data or the VPD policies affecting the table need to be dropped or disabled. The data masking job always drops VPD policies on the tables **Post-masking, you will need to rebuild the VPD policies.** **Tip:** It is recommended to provide the Data Safe user with sufficient privileges to access the table data to ensure the masking job completes successfully. For more information on VPD, see the *Oracle Database Security Guide*.
Data Redaction: The Data Safe user has access or Data Redaction policies are disabled on the tables in the masking policy	Check if the tables being masked have Data Redaction policies applied. In order for the masking job to run properly, the Data Safe user must be granted sufficient privileges to access the table data or the Data Redaction policies affecting the table need to be dropped or disabled. The data masking job always drops Data Redaction policies on the tables. **Post-masking, you will need to rebuild the Data Redaction policies.** **Tip:** It is recommended to provide the Data Safe user with sufficient privileges to access the table data to ensure the masking job completes successfully. For more information on Data Redaction, see the *Oracle Database Data Redaction Guide*.

Table 7-5 (Cont.) Pre-masking checks

Check	Description
Database Vault: The Data Safe user has access or Database Vault policies are disabled on the tables in the masking policy	Check if the Data Safe user has permissions to access the target tables if they are covered by Database Vault policies. In order for the masking job to run properly, the Data Safe must be able to access all the data on the target tables. Ensure that the Data Safe user is granted proper privileges. If Database Vault is not enabled on the table, this check will pass. For more information on Database Vault, see the *Oracle Database Vault Administrator's Guide*.
No active masking jobs on target database	Check if there are active masking jobs on the target database. Masking does not allow concurrent masking jobs on the same target database.
Masking policy contains columns with the deterministic_encryption format with maximum column length less than 27 characters	Check if masking policy contains columns with the `deterministic_encryption` format having maximum column length greater than 27 characters. For more information see, Deterministic Encryption.
`AUTOEXTEND` is disabled for the undo tablespace, but there is still available space remaining	Check whether `AUTOEXTEND` is enabled on UndoTablespace.

If any of the above checks fail, it is recommended to perform the remediation actions listed in the pre-masking report. Once the issues have been remediated, perform the pre-masking check again to determine if the database is properly configured for the masking job. Once all of the checks have passed, you can perform a masking job.

Performing a Pre-masking Check

Prior to initiating a masking job, you must perform a pre-masking check to determine if the database is properly configured for the masking job. If the pre-masking check produces any failures then you should perform the remediation recommendations.

1. Under **Security center**, click **Data masking**.
2. Click **Pre-masking check**.
   The **Pre-masking check** window is displayed.
3. Select a target database. If needed, click **Change compartment** and browse to and select a different compartment.
4. Select a masking policy. If needed, click **Change compartment** and browse to and select a different compartment.
5. (Optional) Enter the tablespace that you want to use for masking if is different than the default tablespace of the Data Safe service account.
6. Click **Submit**.
7. Wait for the pre-masking check to finish. Perform any remediation actions and ensure all checks pass prior to initiating a masking job. This may require running an additional pre-masking check.

> **Note:**
>
> Though it is not recommended, a masking job can be performed even if there are invalid objects.

View a Pre-masking Check Report

After performing a pre-masking check, you will need to view the report to determine if checks were failed or passed. If the pre-masking check produces any failures then you should perform the remediation recommendations.

1. Under **Security center**, click **Data masking**.
2. Under **Related resources**, click **Pre-masking reports**.
3. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
4. (Optional) Under **Filters**, narrow down the scope of reports by selecting a **Policy name**, **Target database**, or entering a **Report name**.
5. From the list of reports, select the one you want to view.

Mask Sensitive Data on a Target Database

You can run a Data Masking job from the **Data Masking** page or the **Masking Policy Details** page.

Mask Sensitive Data from the Data Masking Page

Be sure that you are not trying to mask sensitive data on your production database.

1. Under **Security Center**, click **Data Masking**.
   The **Data Masking** page is displayed.
2. Click **Mask Sensitive Data**.
   The **Mask Sensitive Data** window is displayed.
3. Select a target database. If needed, click **Change Compartment**, and browse to and select a different compartment.
4. Select a masking policy for the selected target database. If needed, click **Change Compartment**, and browse to and select a different compartment.
5. (Optional) Select the tablespace.
6. (Optional) To customize the processing of the masking job for the first time or to override the existing options associated with the selected masking policy, do the following:
   a. Expand **Masking Options**
   b. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.
   c. Specify the value for parallel execution:
      - **NONE** - No parallelism is used when data masking process is running.

- **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
- **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

> **Note:**
>
> The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

d. Specify how you would like invalid objects to recompile after data masking:
   - **NONE** - Invalid objects do not recompile.
   - **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.
   - **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

   > **Note:**
   >
   > If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

e. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

   > **Note:**
   >
   > Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

f. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

7. Click **Mask Data**.
   A warning message states that you should not mask data on a production database.

   The work request page is displayed so that you can see the progress of the masking job.

   You can run only one data masking job at a time on a target database.

Mask Sensitive Data from the Masking Policies Details Page

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of a masking policy to view its details.

The **Masking Policies Details** page is displayed.

4. Click **Mask Target**.
   The **Mask Sensitive Data** page is displayed.
5. Select the target database that you want to mask. If needed, click **Change Compartment**, and browse to and select a different compartment.
6. (Optional) To customize the processing of the masking job for the first time or to override the existing options associated with the selected masking policy, do the following:
   a. Expand **Masking Options**
   b. Disable or enable redo log generation during masking. This is disabled by default. Redo log generation allows you to use a flashback database to retrieve the original unmasked data after it has been masked.
   c. Specify the value for parallel execution:
      - **NONE** - No parallelism is used when data masking process is running.
      - **DEFAULT** - The default value is the optimum number of CPUs to be used in parallel. This is calculated by the Oracle Database.
      - **DEGREE OF PARALLELISM** - Allows you to input an integer to set the number of CPUs to be used in parallel. Refer to the Oracle Database parallel execution framework when choosing an integer value.

      > **Note:**
      >
      > The degree of parallelism is limited by the number of CPUs you have available. If the integer entered in **DEGREE OF PARALLELISM** exceeds the number of available CPUs, it will default to the maximum CPUs available when processing.

   d. Specify how you would like invalid objects to recompile after data masking:
      - **NONE** - Invalid objects do not recompile.
      - **SERIAL**- Invalid objects recompile serially, only when the previous objects has finished compiling.
      - **PARALLEL** - Invalid objects recompile using the same value for parallelism as specified above.

      > **Note:**
      >
      > If a value for parallelism was not specified, the value used will be the optimized value calculated by the Oracle Database.

   e. Enable or disable dropping temporary tables created during data masking after masking is completed. This is enabled by default. Data Masking creates temporary tables that map the original sensitive data values to the mask values. Preserve these table to track how masking changed your data.

> **Note:**
>
> Disabling dropping the temporary tables compromises security. These tables must be dropped before the database is available for unprivileged users.

f. Enable or disable refreshing the statistics gathered on masked database tables after masking. This is enabled by default.

7. Click **Mask Data**.
   A warning message states that you should not mask data on a production database.

   The work request page is displayed so that you can see the progress of the masking job.

   You can run only one data masking job at a time on a target database.

Rerun a Failed Masking Job

If a masking job has failed, you can rerun the masking job from the failed step, pre masking script, or post masking script. The masking job will start from the step you select and continue through the rest of the masking job.

1. Under **Security center**, click **Data masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Select the masking policy for the failed masking job.
4. Under **Additional details** in the **Masking policy information** tab, click **Work request: View details**.
5. Click **Rerun**.
6. Select which step you would like the masking job to rerun from.
   The masking job will start from the step you select and continue through the rest of the masking job.
7. Click **Rerun**.

View and Analyze Data Masking Reports

After you run a data masking job, Oracle Data Safe saves all the details about the data masking job in Security Center as an online report and tracks statistics across the top five masking policies for a target database.

Statistics About a Masked Target Database

The following information is available in Data Masking for a masked target database:

- The number of masking policies created for a target database and their names
- Statistics across all policies for a target database: Includes the number of masked sensitive types, schemas, tables, columns, and values
- Charts comparing the percentage of masked values and percentage of masked columns for the top five masking policies.
- Statistics per masking policy: Includes the number of reports available, masked sensitive types, schemas, tables, columns, and values

- Details and statistics for each data masking job: Includes the target database name, masking policy name, report Oracle Cloud Identifier (OCID), the start and finish date/time of the data masking job, and the number of masked sensitive types, schemas, tables, columns, and values. For each column, the schema name, table name, masking format used, sensitive type, parent column, and total number of masked values is provided. Log files are available for the data masking job.

View and Analyze Masked Data for a Target Database

1. Under **Security center**, click **Data masking**.
2. On the **Masked target databases** tab, click the name of the target database for which you want to view the Data Masking report.

   Notice that the **Masking policies** column tells you how many masking policies exist for the target database.
3. On the **Masking summary** tab, view statistics across all masking policies for the target database.

   You can view the number of masked sensitive types, schemas, tables, columns, and values. There are two charts included. The first chart compares the percentage of masked values for the top five masking policies. The second chart compares the percentage of masked columns for the top five masking policies.
4. In the **Masking polices** section, view the list of masking policies for the target database.

   Notice that the **Masking reports** column tells you how many reports exist for each masking policy.
5. In the **Masking reports** column, click the numerical link for a masking policy report.
6. On the **Masking summary** tab, view statistics for the latest data masking job.

   You can view the target database name, the masking policy name, and the number of masked sensitive types, schemas, tables, columns, and values.
7. In the **Masking reports** section, you can view totals for each masking job, including the number of masked sensitive types, schemas, tables, columns, and values.

   The **Report time** column provides a link to each Data Masking report.

   Notice that each report is named according to its date and time.
8. In the **Report time** column, click the link to a Data Masking report.

   The **Masking report** page is displayed.
9. On the **Masking report information** tab, view details and statistics for the data masking job.

   Details include the target database name, masking policy name, report OCID (Oracle Cloud Identifier), and the start and finish date/time of the data masking job. Statistics included are the number of masked sensitive types, schemas, tables, columns, values, and the number of pre and post masking errors.
10. In the **Masked columns** section, view the details about each masked column. For each column, the schema name, table name, masking format used, sensitive type, parent column, and total number of masked values is provided.
11. To view the data masking errors, under **Resources**, click **Masking errors**.

    The **Masking errors** section lists the errors, what step they occurred in, and the time they occurred.

12. To view the data masking job logs, under **Resources**, click **Masking logs**.

    The **Masking logs** section lists the log messages and when they occurred.

Download Data Masking Reports

You can download a data masking report as a PDF or XLS file. You first need to generate the report before you can download it. Generate the report in the file format that you wish to download.

About Data Masking Reports

Data Masking reports contains the following sections and information:

- **Report header:** Shows the masking policy name, target database, and report time (in UTC time).
- **Summary table:** Shows the total number of sensitive categories, sensitive types, tables masked, columns masked, and values masked.
- **Masked Columns table:** Lists each column and its sensitive category, sensitive type, schema name, table name, masking format used, and the total number of masked values.

The following is an example of a PDF version of a Data Masking report:

The following is the same report in XLS format:

Generate a Data Masking Report

1. Under **Security Center**, click **Data Masking**.
2. On the **Masked Target Databases** tab, click the name of the target database for which you want to generate the Data Masking report.
3. In the **Masking Reports** column, click the numerical link for the report.
4. In the **Report Time** column, click the link to the Data Masking report that you want to generate.

   The **Masking Report** page is displayed.
5. Click **Generate Report**.

   The **Generate Report** dialog box is displayed.
6. Select **PDF** or **XLS**, and then click **Generate Report**.
7. Wait for the message that says the report generation is complete, and then click **Close**.

Download a Data Masking Report

1. Under **Security Center**, click **Data Masking**.
2. On the **Masked Target Databases** tab, click the name of the target database for which you want to download the Data Masking report.
3. In the **Masking Reports** column, click the numerical link for the report.
4. In the **Report Time** column, click the link to the Data Masking report that you want to download.

The **Masking Report** page is displayed.

5. Click **Download Report**.

   The **Download Report** dialog box is displayed.

6. Select **PDF** or **XLS**, depending on the file format selected when you generated the report, and then click **Download Report**.

   A dialog box is displayed with the option to open the downloaded file or save it to your local computer.

7. To open the file, select **Open with**, select an application that can open the file format, and then click **OK**.

8. To save the file to your local computer, leave **Save File** selected, and then click **OK**. In the **Enter name of file to save to** dialog box, browse to a directory, enter a file name, and then click **Save**.

Delete a Data Masking Report

1. Under **Security Center**, click **Data masking**.
2. On the **Masked Target Databases** tab, click the name of the target database for which you want to delete the data masking report.
3. In the **Masking reports** column, click the numerical link for the report.
4. In the **Report Time** column, click the link to the data masking report that you want to delete.

   The **Masking report** page is displayed.

5. Click **Delete report**.
6. Click **Delete**

Download or Upload Masking Policies in XML Format

You can download an XML version of a masking policy and upload it into Oracle Data Safe, replacing an existing masking policy or creating a new one. Before downloading a masking policy, you first need to generate it as an XML file.

About Downloading and Uploading Masking Policies

There are several use cases for downloading and uploading masking policies. For example:

- You have multiple test databases in different regions in Oracle Cloud Infrastructure, all with the same schemas, and you want to mask them all the same way.
- Your test database has moved to another region in Oracle Cloud Infrastructure and you want to move the masking policy with it.
- Your masking policy is large and complex so you prefer to manually edit it in a text editor instead of going through the Data Masking interface.

Generate a Masking Policy in XML Format

1. Under **Security Center**, click **Data Masking**.

2. Under **Related Resources**, click **Masking Policies**.

   The **Masking Policies** page is displayed.

3. Search for and click the masking policy that you want to download.

   The **Masking Policy Details** page is displayed.

4. Click **Generate Policy**.

   The **Generate Masking Policy for Download** is displayed.

5. Click **Generate Policy** and wait for the XML file to be generated.

   A message states the XML file generation is complete. You can download it using the **Download Policy** button.

6. Click **Close**.

Download a Masking Policy in XML Format

You need to first generate the masking policy before you can download it.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.

   The **Masking Policies** page is displayed.

3. Search for and click the masking policy that you want to download.

   The **Masking Policy Details** page is displayed.

4. Click **Download Policy**.

   The **Download Masking Policy** dialog box is displayed.

5. Click **Download Policy**.

   The **Opening Policy-download.xml** dialog box is displayed.

6. Either open the XML file with a selected application or leave **Save File** selected, and click **OK**. If you choose to save the file, browse to a location on your local computer, enter a file name, and click **Save**.

Upload a Masking Policy in XML Format

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.

   The **Masking Policies** page is displayed.

3. Click **Upload Masking Policy**.

   The **Upload Masking Policy** page is displayed.

4. To replace an existing masking policy, do the following:

   a. Leave the **Update an existing masking policy** tile selected.

   b. Select the masking policy that you want to replace. If needed, click **Change Compartment** and select a different compartment.

   c. Add your masking policy. There are two ways to do this. The first way is to drag your masking policy file (XML file) onto the **Upload Masking Policy File** area. The second

way is to click **select one**, browse to and select your XML file in the **File Upload** dialog box, and then click **Open**.

d. Click **Upload Masking Policy**.

5. To create a new masking policy using the XML file, do the following:

a. Select the **Create a new masking policy** tile.

b. Enter a name for your new masking policy.

c. Select the compartment where you want to store your masking policy.

d. (Optional) Enter a description for your masking policy.

e. Choose how you want to create the masking policy, either associating it with a Sensitive Data Model or with a Target Database. When using a sensitive data model, select the sensitive data model from the drop down menu. When using a target database, select the target database from the drop down menu.

f. Add your masking policy. There are two ways to do this. The first way is to drag your masking policy file (XML file) onto the **Upload Masking Policy File** area. The second way is to click **select one**, browse to and select your XML file in the **File Upload** dialog box, and then click **Open**.

g. (Optional) To add tags, click **Show Advanced Options**, and create tags.

h. Click **Upload Masking Policy**.

It's important to leave the window open during the upload process.

Manage Masking Formats and Masking Policies

You can move user-defined masking formats and masking policies to different compartments and delete them as needed. You cannot delete Oracle predefined masking formats.

Change Target Database of a Masking Policy

Learn how to edit the target database of an existing masking policy.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the name of your masking policy to view its details.

   The **Masking Policies Details** page is displayed. The **Masking Policy Information** tab shows you the name and Oracle Cloud Identifier (OCID) of your masking policy, the work request information, the compartment in which the masking policy is stored, the target database with which the masking policy is associated, the name of the sensitive data model, and when the masking policy was created and last updated.
4. Change the target database associated with the masking policy by clicking the pencil icon next to the **Target Database** field.

   The **Change Target Database** dialog will appear.
5. (Optional) change the compartment by selecting **Change Compartment**. Select the new compartment from the list.
6. Select the new target database from the target database drop-down list.
7. Click **Submit**.

Move a Masking Format or Masking Policy to a Different Compartment

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats** or **Masking Policies**.
3. Search for and click the name of the masking format or masking policy that you want to move.

   The **Masking Format Details** page or the **Masking Policy Details** page is displayed.
4. Click **Move Resource**.

   The **Move Resource to a Different Compartment** dialog box is displayed.
5. Select a different compartment, and then click **Move Resource**.

   The masking format or masking policy is immediately moved to the selected compartment.

Delete a User-Defined Masking Format or Masking Policy

Deleting a masking format is permanent and cannot be undone.

1. Under **Security Center**, click **Data Masking**.
2. Under **Related Resources**, click **Masking Formats** or **Masking Policies**.
3. Search for and click the name of the masking format or masking policy that you want to delete.

   The **Masking Format Details** page or the **Masking Policy Details** page is displayed.
4. If you want to delete a masking format, click **Delete**. If you want to delete a masking policy, from the **More Actions** menu, select **Delete**.

   A **Confirm** dialog box is displayed, asking you to confirm the deletion.
5. Click **Delete**.

   The user-defined masking format or masking policy is immediately deleted.

Create and Modify Event Notifications in Data Masking

You can create and modify event notifications in Data Masking.

Creating Event Notifications for Data Masking

In Data Safe you can create event notifications for Data Masking related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **Data masking**.

2. Under **Related Resources**, click **Masking Policies**.
3. Click the **Notifications** tab.
4. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
5. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

6. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See Data Masking Event Types in the *Administering Oracle Data Safe* guide for more information on events.
7. Select to either **Create new topic** or to **Select existing topic**.
8. Select a **Compartment**.

   > **Note:**
   >
   > This compartment is where the topic will be created, not where the rule and event will be monitored in.

9. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
10. Select a **Subscription protocol**.
11. Provide the necessary inputs for the selected subscription protocol.
12. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
13. Click **Create notification**.

Modifying Event Notifications For Data Masking

After creating event notifications in Data Masking in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **Data masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the **Notifications** tab.
4. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **Data masking**.
2. Under **Related Resources**, click **Masking Policies**.
3. Click the **Notifications** tab.
4. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

8

SQL Firewall

This section discusses how to protect your Oracle Databases (23ai and above) from common database attacks such as SQL injection and credential theft or abuse by using the SQL Firewall feature in Oracle Data Safe.

SQL Firewall Overview

The SQL Firewall feature in Oracle Data Safe lets you administer and monitor SQL Firewall across your fleet of Oracle Database 23ai targets.

About SQL Firewall

The SQL Firewall feature in Oracle Data Safe lets you administer and monitor SQL Firewall across your fleet of Oracle Database targets. SQL Firewall is a new security feature built into the Oracle Database 23ai kernel and offers protection against risks such as SQL injection attacks and compromised accounts. SQL Firewall inspects all incoming database connections and SQL statements, including the ones from PL/SQL units, whether local or over the network, encrypted or clear text. It only allows explicitly authorized SQL and can log or block SQL statements and connections that do not fall within the SQL Firewall allowlists.

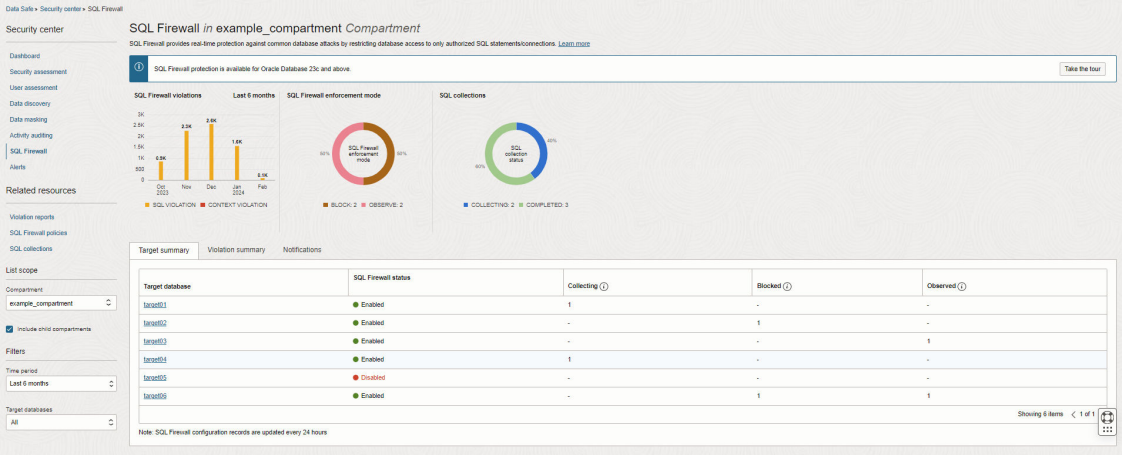
SQL Firewall uses allowlists of authorized SQL statements and trusted database connection paths to determine which SQL statements and connection paths are authorized and which ones should be either logged or blocked. SQL Firewall allowlist policies work at a database account level. You create an SQL Firewall allowlist for a database account by capturing or collecting the expected application SQL workload from expected database connections. Subsequently, the firewall detects and prevents unauthorized SQL and potential SQL injection attacks.

To learn more about SQL Firewall in Oracle Database see the *Oracle Database Oracle SQL Firewall Guide*

SQL Firewall can be managed in multiple ways. The PL/SQL procedures in `SYS.DBMS_SQL_FIREWALL` package lets you manage SQL Firewall directly in an Oracle Database (23ai or above). Consider Oracle Data Safe if you are looking forward to leveraging the convenience of the Oracle Cloud Infrastructure (OCI) ecosystem and want to manage and monitor SQL Firewall for a fleet of Oracle Database targets.

Administrators can use Data Safe to collect SQL activities of database accounts, monitor the collection progress, create SQL Firewall policies with allowlist rules (allowed contexts and allowed SQL statements) from the collected SQL activities, and enable SQL Firewall policies. Once a SQL Firewall policy is enabled, Data Safe automatically collects the firewall violation logs from the database and stores them in Data Safe. Those logs are then available for online analysis and reporting across your database fleet as shown in Figure 8-1. You can leverage the Data Safe REST APIs, SDKs, CLI, and Terraform for further automation and integration. You can also leverage the larger OCI ecosystem for integrating SQL Firewall violations with its alerts and notifications.

Figure 8-1 SQL Firewall dashboard in Data Safe



Terms in SQL Firewall

The following terms are used throughout Oracle Data Safe's SQL Firewall feature.

- Database security configuration - This resource represents the target database configurations. Included in the Database security configurations are the SQL Firewall configurations such as the status of the firewall, the time that the firewall status was last updated, violation log auto purge settings, and so on.
- Session context - This represents client information initiating SQL traffic: client IP address, OS program name, and OS username.
- SQL collection - This resource represents the SQL collection for a specific database user in a target database. SQL collection encapsulates the SQL commands issued in the user's database sessions and their session context.
- SQL Firewall policy - An allowlist policy specific to a database user through which incoming SQL statements will be evaluated to determine if they can take action on the target database. SQL statements can be allowed or, if they're not part of the allowlist, allowed and logged or blocked and logged. The policy can consist only of session context information, only of specific SQL statements, or both.
- SQL violations - This represents SQL statements that were initiated on the target database that are not included in the allowlist in the SQL Firewall policy.
- Context violations - This represents session context from which SQL statements were initiated on the target database that are not included in the allowlist in the SQL Firewall policy.
- Observe and log violations - A SQL Firewall policy enforcement option where initiated SQL statements that are either SQL or context violations are allowed to execute on the target database and the statements and context are logged for later reference.
- Block and log violations - A SQL Firewall policy enforcement option where initiated SQL statements that are either SQL or context violations are blocked and can't execute on the target database. The statements and context are logged for later reference.

Prerequisites for SQL Firewall

SQL Firewall requires you to register an Oracle Database 23ai target database in Data Safe. Users must be granted specific permissions in IAM.

These are the prerequisites for using the SQL Firewall feature in Data Safe:

- Register an Oracle Database 23ai or later. For more information see, Target Registration in the *Administering Oracle Data Safe* guide.
- Grant the SQL Firewall role to the Data Safe service account on the target database. For more information, see Roles for the Oracle Data Safe Service Account in the *Administering Oracle Data Safe* guide.
- Obtain the required IAM permissions which can be granted by a tenancy administrator: To use the full functionality of SQL Firewall it is recommended to be granted `manage` permissions on `data-safe-sql-firewall-family` in the relevant compartments.

  ```
  Allow group <group-name> to manage data-safe-sql-firewall-family in
  compartment
          <compartment-name>
  ```

  Alternatively, administrators may grant more selective permissions by granting permissions to specific resources within `data-safe-sql-firewall-family`. For more information on the resources contained within `data-safe-sql-firewall-family`, see `data-safe-sql-firewall-family` Resource.

Start Using SQL Firewall

In order to begin using SQL Firewall you need to complete the following steps. Ensure you have already completed the prerequisites before starting these steps.

These steps will walk you through

1. Enabling SQL Firewall on your Oracle Database 23ai or above
2. Collecting SQL traffic
3. Stopping the collection of SQL traffic
4. Generating and enforcing SQL Firewall policies
5. Viewing SQL Firewall violation logs
6. Creating audit trails and alert policies for SQL Firewall violations
7. Configuring notifications for SQL Firewall violations

By completing these steps you will be taking steps to protect your database fleet against SQL injection attacks and compromised accounts.

Step 1: Enable SQL Firewall On Your Target Database

This steps ensures that SQL Firewall is enabled on your target database.

1. Under **Security center**, click **SQL Firewall**.

2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Click **Enable**. This can be done through either the button under the name of the database security configuration or the Enable option under the Target database section of the Database security configuration information tab.
6. Wait for the resource to change to Active before continuing to the next step.

Step 2: Start SQL Collection for a Database User

This step starts the collection of expected SQL statements and expected database connection paths for the database user. Run the typical application workload from the trusted database connection paths.

1. In the Configuration details page from the previous step, click **Create and start SQL collection.**
2. Select the database user for which collection needs to be created.
3. Select the SQL Collection Level:
   - User issued SQL commands - These are SQL statements that were issued directly from the user to be executed on the database. This is the default.
   - User issued SQL commands and SQL commands issues from PL/SQL units - This includes SQL statements issued directly from the user as well as SQL statements within a PL/SQL unit which is invoked by the user.

     Note: SQL collection will *not* record any internal recursive SQL statements.
4. Click **Create and start SQL collection.**
5. Perform typical daily tasks in your applications for the selected database user.
6. Allow the SQL collection to run for some time. This is discussed further in Step 3: Monitor the Progress of SQL Collection with Insights.

Step 3: Monitor the Progress of SQL Collection with Insights

In this step you will monitor the collection of SQL statements and determine when collection can be stopped. Monitor the SQL collection until you see there are no new incoming unique SQL statements or trusted connection paths from the running workload.

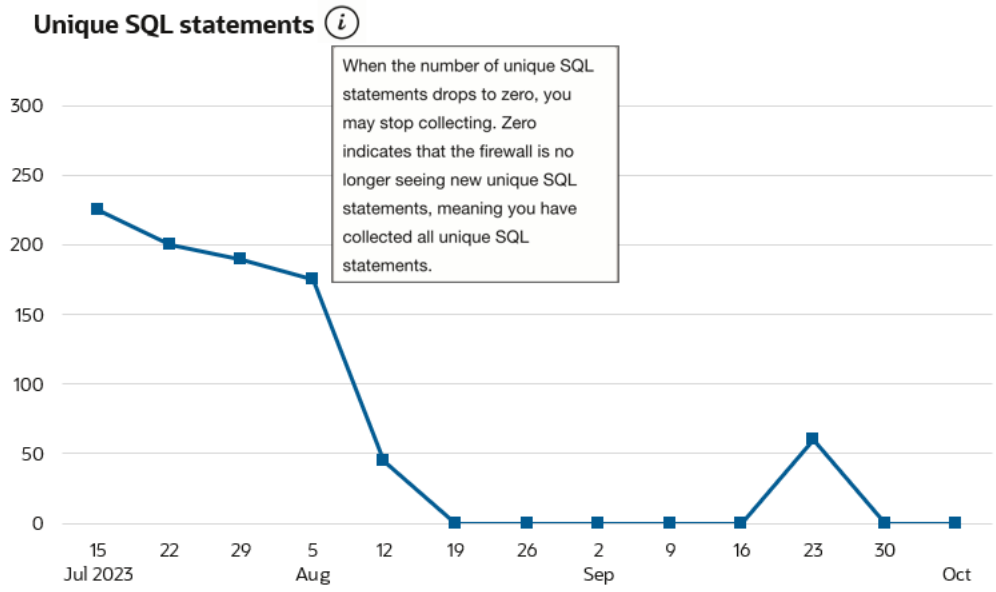
1. Click the **SQL collection insights** tab.
2. The information on the SQL collection tab refreshes every hour, if necessary click **Refresh Insights**.
3. (Optional) Select the time period for which you would like to review the SQL collection.
4. Review the Unique SQL statements chart.
   The collected SQL statements are analyzed to determine if they are unique over the span of the collection period and this chart displays the number of unique SQL statement on the

selected time interval. Once there are no more new unique SQL statement being initiated, i.e. the chart remains steady at zero, it is recommended to stop the collection. Waiting until the number of unique SQL statements comes to zero ensures that you collect all statements that are typically executed on your target database and helps establish a status quo.

For example, if there are 250 SQL statements executed on the first day of the collection but only 225 of those are unique then the chart will show 225 for that day. In the following week if the same 250 statements and an additional 200 new and unique statements are executed then the chart will only show 200. This is because the 250 statements were already collected and observed in week one, thus they are not unique. The number of unique SQL statements will reach zero when there are no more unique SQL statements are observed. See Figure 8-2 for reference.

It may take several days to weeks for you to collect enough unique SQL statements to stabilize at zero.

Figure 8-2 Unique SQL Statements chart in SQL Collection Insights



5. Review the Client IP, Client OS user, and Client program charts.
These charts show you the number of client IP addresses, OS users, and programs, respectively, that are executing SQL commands on your target database each day. The specific context information can be viewed in the table below the charts.

   Since SQL statements should be coming from the same session contexts each day, it is recommended to stop the collection when the charts stabilize at a certain value day to day.

6. Review the list of session context types and values.
Reviewing the list of client IP addresses, client OS users, and client programs allows you to determine where your traffic is coming from. With this information you can set up rules that log or block traffic from all other locations. This is further discussed in Step 4: Generate and Enforce SQL Firewall Policies.

7. Once you have collected a sufficient amount of unique SQL statements, click **Stop** to stop the collection.
Once you have stopped the collection you will see start time, stop time, and the elapsed time under **Collection timeline** of the **SQL collection information** tab.

Step 4: Generate and Enforce SQL Firewall Policies

In this step you will review the information gathered during the collection and create policies with allowlists based on the collected data. Policies will also be enforced to either observe and allow violations or block violations.

1. In the SQL collection details page from the previous step, click **Generate firewall policy.**This will take you to the Firewall policy details page.
2. Review the SQL session context and the Unique allowed SQL statements tables.
   If desired you can add, edit, or remove session context information to be included in the policy but you can't add, edit, or remove any of the collected unique SQL statements in the policy.
3. (Optional) Update the allowed SQL session context values as desired.
   a. Click **Update** for the respective row.
   b. To remove a value, click the **X** at the end of the row in the panel.
   c. To add a value, click **Add** and enter the new value in the empty field.
   d. Click **Update client IP/client program/client OS user**, depending on which context information you selected.
4. (Optional) Download a PDF or XLS report of all Unique allowed SQL statements.
   a. Click **Generate report**.
      A pop-up will appear.
   b. Select which format you want the report in, PDF or XLS.
   c. Enter a name for the report.
   d. Optionally, enter a description for the report.
   e. Click **Generate report**.
   f. Download the report. You have two options:
      - In the Generate report window, click the **here** link. The document will begin downloading.
      - Click **Close** to close the Generate report window. Then, click the **Download report** button. A dialog box is displayed providing you options to open or save the document.
5. Click on **Deploy and Enforce**.
   a. Select the enforcement scope:
      - All (Session contexts and SQL statements)
      - Session contexts only - This option enforces the checks only on the database connection paths.
      - SQL statements only - This option enforces the checks only on the SQL statements.
   b. Select the action on violations:
      - Observe (Allow) and log violations - This option will observe and allow all SQL statements and connections to the database while logging any violations.

- Block and log violations - This option will block any SQL statements and database connections not listed in the policy and log the violations. Consider this option when you want SQL Firewall to prevent unauthorized SQL traffic to the database.

c. Audit for violations

- On - This option will write the violation records to the audit trail. It enables alerting and helps demonstrate compliance to your audit requirements. Ensure to start the audit trail in Data Safe to collect the audit events. These audit events contribute to the monthly free limit of 1 million audit records per month per target database.
- Off

d. Click **Deploy and enforce**.

Step 5: View SQL Firewall Violation Reports

In this step you can view a report of violations for your enforced SQL Firewall policies. There are a variety of ways to navigate to the violations report, some of which will automatically apply filters for your selected SQL Firewall policies, target databases, time periods, and so on.

> **Note:**
>
> It is unlikely that you will see any violations immediately after enforcing a SQL Firewall policy.

- View all violations
- View target specific violations
- View policy specific violations

View all violations

Complete these steps to view a report of all violations across your database fleet.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation reports.**
3. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
4. Select which report you would like to see from the **Predefined reports** tab:
   - All violations report - Both SQL and context violations
   - SQL violations report - Violations on SQL statements
   - Context violations report - Violations on database connection paths
5. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters
   - Apply advanced SCIM filters
   - Create custom reports

- Schedule reports
- Generate and download reports
- Manage which columns to display

View target specific violations

Complete these steps to view a report of all violations on a specific target database from the last week.

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Violation summary** tab.
3. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
4. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
5. Select the name of a target database from the list.
   This will take you to the violation report.
6. The violation report will be automatically filtered to show only the violations for the selected target database from the selected time period.
7. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters
   - Apply advanced SCIM filters
   - Create custom reports
   - Schedule reports
   - Generate and download reports
   - Manage which columns to display

View policy specific violations

Complete these steps to view a report of violations specific to a selected SQL Firewall policy.

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Select the name of a target database from the list on the **Target summary** tab.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Firewall policies**.
6. Select a SQL Firewall policy from the list.
   This will take you to the Firewall policy details page.

7. Under **Enforcement information**, click **View report** next to **Violation reports**.
8. The violation report will be automatically filtered to show only the violations for the selected database user on the selected target database.
   This will take you to the violation report.
9. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters
   - Apply advanced SCIM filters
   - Create custom reports
   - Schedule reports
   - Generate and download reports
   - Manage which columns to display

Step 6 (Optional): Create Audit and Alert Policies for SQL Firewall Violations

In this step you will create audit and alerts policies for SQL Firewall violations so that you can better track and monitor activity on your database fleet. Though this step is optional, it is recommended as it enables alerting and helps demonstrate compliance to your audit requirements.

Complete the prerequisites for Activity Auditing and Alerts.

1. Complete the Activity Auditing workflow to audit SQL Firewall violations.
   You need to have turned on **Audit for violations** when enforcing your SQL Firewall policies for the corresponding audit policies to show as enabled in Activity auditing. You can view and manage the audit policies for SQL Firewall listed under the SQL Firewall auditing section of the Audit policy details.

   > **Tip:**
   >
   > You must turn on **Audit for violations** in your SQL Firewall policy before managing the SQL Firewall audit policies in the Activity Auditing workflow. See Update the Enforcement of SQL Firewall Policies for more information.

2. Complete the Alerts workflow to receive alerts for SQL Firewall violations.
   The alert policy for SQL Firewall is **SQL Firewall violations**.

Step 7 (Optional): Configure Notifications for SQL Firewall Violations

In this step you will configure notifications for when a SQL Firewall violation occurs. Though this step is optional, it is recommended as it will enable you to receive near real-time alerts in the event of a SQL Firewall violation.

In Data Safe you can create event notifications through a workflow available in SQL Firewall. This allows you to create event notifications in context. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Notifications** tab.
3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

   > **Note:**
   >
   > The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**.
   If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See SQL Firewall Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

   > **Note:**
   >
   > This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.

b. Select a **Tag Namespace** from the drop-down list.

c. Provide a **Tag Key** and **Tag Value**.

12. Click **Create notification**.

Following the completion of these steps, SQL Firewall will start observing the incoming SQL statements and database connection paths, and will allow or block the SQL traffic to proceed to the target database based on the enforced SQL Firewall policy while logging any violations. You can monitor the SQL Firewall violations in Data Safe. If you configured audit and alert configuration, OCI notifications will be triggered in the event of a SQL Firewall violation.

Gain Insights from SQL Firewall

After successfully setting up SQL Firewall to monitor and block and allow SQL activity on your Oracle Database 23ai target databases, you'll want to ensure that you understand the dashboard and violations report. You should also understand what actions to take in the event of a high volume of violations.

View the SQL Firewall Dashboard

When you select **SQL Firewall** under **Security center** in Oracle Data Safe you will see the dashboard of SQL Firewall information for the last week. This dashboard provides you with a high-level view of your SQL Firewall implementation across your fleet of Oracle Database 23ai or above target databases in your selected compartment(s).

To filter the dashboard you can alter the compartments, time period, and databases that you can see information for by:

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.

The dashboard shows the following information:

- **SQL Firewall violations** chart - Shows the number of SQL statement violations and the number of context violations throughout your Oracle Database 23ai or above fleet per day. This allows you to determine patterns in the number of SQL statement and session context violations and identify spikes in violations that should be investigated.
- **SQL Firewall enforcement mode** chart - Shows you a break down of how many of your SQL Firewall policies either "block" or "observe" SQL statements or session contexts that violate your policies.
- **SQL Collections** chart - Shows you a break down of the number of SQL collections in each life cycle state: `COLLECTING`, `COMPLETED`, `DELETED`, `FAILED`, `NEEDS_ATTENTION`.
- **Target Summary** tab - Shows you a break down per registered Oracle Database 23ai or above of the number of database users that SQL statements are actively being collected for, the number of policies that block violations, and the number of polices that allow and observe violations. You can click on the name of a target database to see its SQL Firewall configuration details and drill down deeper into the SQL collections, SQL Firewall policies, and Work Requests on the target database.

- **Violations Summary** tab - Shows you a break down per registered Oracle Database 23ai or above of the total number of violations, the number of SQL violations, and the number of Context violations. You can click on the name of a target database to see a more detailed violations report.
- The **Notifications** tab - Shows you what event notifications and subscriptions you have created for SQL Firewall. More specifically, it displays the event, rule name, topic name, and when the event notification was created. This table will only show Events that you have created directly within Data Safe. In addition to displaying existing event notifications, you can also create new notifications by using the Create notification button. See Create and Modify Event Notifications in SQL Firewall for more information.

View Violations

There are multiple ways that you can view context and SQL statement violations once you have enforced SQL Firewall policies.

View all violations

Complete these steps to view a report of all violations across your database fleet.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation reports.**
3. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
4. Select which report you would like to see from the **Predefined reports** tab:
   - All violations report - Both SQL and context violations
   - SQL violations report - Violations on SQL statements
   - Context violations report - Violations on database connection paths
5. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters
   - Apply advanced SCIM filters
   - Create custom reports
   - Schedule reports
   - Generate and download reports
   - Manage which columns to display

View target specific violations

Complete these steps to view a report of all violations on a specific target database from the last week.

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Violation summary** tab.
3. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
4. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
5. Select the name of a target database from the list.
   This will take you to the violation report.
6. The violation report will be automatically filtered to show only the violations for the selected target database from the selected time period.
7. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters
   - Apply advanced SCIM filters
   - Create custom reports
   - Schedule reports
   - Generate and download reports
   - Manage which columns to display

View policy specific violations

Complete these steps to view a report of violations specific to a selected SQL Firewall policy.

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Select the name of a target database from the list on the **Target summary** tab.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Firewall policies**.
6. Select a SQL Firewall policy from the list.
   This will take you to the Firewall policy details page.
7. Under **Enforcement information**, click **View report** next to **Violation reports**.
8. The violation report will be automatically filtered to show only the violations for the selected database user on the selected target database.
   This will take you to the violation report.
9. Once at the report you may perform all standard report actions in Oracle Data Safe such as:
   - Apply basic filters

- Apply advanced SCIM filters
- Create custom reports
- Schedule reports
- Generate and download reports
- Manage which columns to display

Related Topics

- View and Manage Violations Report
  Describes actions that can be take on reports and how to create custom reports.

Follow-Up Actions for SQL Firewall

In an ideal scenario where the SQL collection has captured all expected SQL statements and trusted database connections, violations indicate potential database attacks such as compromised account access and SQL Injection attacks. But if the collected statements or database connections are not complete or there are new authorized SQL statements following an application update, there is a possibility to see a surge in violations. Ensure to update the SQL Firewall policies to collect these additional statements to avoid false positives in the violation reports.

Related Topics

- Update SQL Firewall Policies

Manage SQL Firewall

Managing your SQL Firewall policies and configurations helps ensure that your databases are protected from threats while also ensuring that intended SQL actions can be taken on your databases. See the below topics for information on how to update your SQL Firewall configurations and policies.

Update the Database Security Configuration

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Perform any of the following tasks:
   - Click **Disable** next to **SQL Firewall status** to disable SQL Firewall. This will stop any ongoing collections and policies will no longer be enforced.

- Click **Turn on** or **Turn off** next to **Auto-purge violation logs** to turn this on or off. This specifies whether Data Safe should automatically purge the violation logs from the database after collecting the violation logs and persisting them on Data Safe.

  > **Note:**
  >
  > When this is turned on violation logs are automatically purged every seven days.

- Click **Include** or **Exclude** next to **Database jobs** to include or exclude database jobs for SQL Firewall enforcement.
- Click **Refresh** next to **Last refresh time** to refresh Data Safe's copy of the policies if you made a recent policy change within the database.
- Click **Move Resource** to move the Database Security Configuration to a different compartment.

Purge a SQL Collection

Purge helps clean the collection logs for the user. You typically need to purge the SQL Collection when you need to recapture an application SQL workload for the same database user following application updates. The SQL collection can be started again for the database user once it is purged.

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL collections**.
6. Click on a database user name.
   This will take you to the SQL collection details page.
7. Click **Purge** to remove the SQL collection. This will not stop any SQL Firewall Policies that were generated from this collection.

Drop a SQL Collection

Drop will remove the SQL Collection and collection logs for the selected database user. You typically have to drop the SQL Collection when you need to remove SQL Firewall protection for a database user who is no longer active or has changed responsibilities in the system.

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:

a. (Optional) Select a time period from the **Time period** menu.

b. (Optional) Select a target database from the **Target database** menu.

4. Click on the name of a target database.
This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Collections**.
6. Click on a database user name.
This will take you to the SQL collection details page.
7. Click on **More actions** and select **Drop** to delete the SQL collection. Dropping a SQL collection will not have an impact on already generated or enforced SQL Firewall policies.

View and Manage SQL Firewall Policies

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:

a. (Optional) Select a time period from the **Time period** menu.

b. (Optional) Select a target database from the **Target database** menu.

4. Click on the name of a target database.
This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Firewall policies**.
6. Click on a database user name.
This will take you to the Firewall policy details page.
7. (Optional) Update the allowed SQL session context values as desired.

a. Click **Update** for the respective row.

b. To remove a value, click the **X** at the end of the row in the panel.

c. To add a value, click **Add** and enter the new value in the empty field.

d. Click **Update client IP/client program/client OS user**, depending on which context information you selected.

8. (Optional) Download a PDF or XLS report of all Unique allowed SQL statements.

a. Click **Generate report**.
A pop-up will appear.

b. Select which format you want the report in, PDF or XLS.

c. Enter a name for the report.

d. Optionally, enter a description for the report.

e. Click **Generate report**.

f. Download the report. You have two options:

- In the Generate report window, click the **here** link. The document will begin downloading.
- Click **Close** to close the Generate report window. Then, click the **Download report** button. A dialog box is displayed providing you options to open or save the document.

Update SQL Firewall Policies

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL collection**.
6. Click on a database user name.
   This will take you to the SQL collections details page.
7. Click on the associated SQL Firewall policy located in the SQL collection information tab.
   This will take you to the Firewall details page.
8. Temporarily disable the SQL Firewall policy by clicking **Disable**. Confirm disablement in the pop-up by clicking **Disable**.
9. Navigate back to the SQL collection by clicking **SQL collection details** in the page breadcrumbs.
10. Click **Start** to capture SQL statements.
11. Initiate the SQL statements you want to add on your target database.
12. Click **Stop** once you have collected the SQL statements.
13. Click **Update firewall policy** to append the new SQL statements to the associated policy.
14. Click on the associated SQL Firewall policy located in the SQL collection information tab.
    This will take you to the Firewall details page.
15. Click on **Deploy and Enforce**.
    a. Select the enforcement scope:
       - All (Session contexts and SQL statements)
       - Session contexts only - This option enforces the checks only on the database connection paths.
       - SQL statements only - This option enforces the checks only on the SQL statements.
    b. Select the action on violations:
       - Observe (Allow) and log violations - This option will observe and allow all SQL statements and connections to the database while logging any violations.
       - Block and log violations - This option will block any SQL statements and database connections not listed in the policy and log the violations. Consider this option when you want SQL Firewall to prevent unauthorized SQL traffic to the database.
    c. Audit for violations
       - On - This option will write the violation records to the audit trail. It enables alerting and helps demonstrate compliance to your audit requirements. Ensure to start the

audit trail in Data Safe to collect the audit events. These audit events contribute to the monthly free limit of 1 million audit records per month per target database.

- Off

d. Click **Deploy and enforce**.

Update the Enforcement of SQL Firewall Policies

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Firewall policies.**
6. Select a SQL Firewall policy from the list.
   This will take you to the Firewall policy details page.
7. Click on **Deploy and Enforce**.
   a. Select the enforcement scope:
      - All (Session contexts and SQL statements)
      - Session contexts only - This option enforces the checks only on the database connection paths.
      - SQL statements only - This option enforces the checks only on the SQL statements.
   b. Select the action on violations:
      - Observe (Allow) and log violations - This option will observe and allow all SQL statements and connections to the database while logging any violations.
      - Block and log violations - This option will block any SQL statements and database connections not listed in the policy and log the violations. Consider this option when you want SQL Firewall to prevent unauthorized SQL traffic to the database.
   c. Audit for violations
      - On - This option will write the violation records to the audit trail. It enables alerting and helps demonstrate compliance to your audit requirements. Ensure to start the audit trail in Data Safe to collect the audit events. These audit events contribute to the monthly free limit of 1 million audit records per month per target database.
      - Off
   d. Click **Deploy and enforce**.

Disable or Enable SQL Firewall Policies

1. Under **Security center**, click **SQL Firewall**.

2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Under **Resources,** click **SQL Firewall policies.**
6. Select a SQL Firewall policy from the list.
   This will take you to the Firewall policy details page.
7. Click **Disable** or **Enable**. Disabling will stop the SQL Firewall from evaluating any incoming SQL traffic against this SQL Firewall policy. However, this will not delete the policy and it can be enabled again later.

Drop SQL Firewall Policies

1. Under **Security center**, click **SQL Firewall**.
2. (Optional) Under **List scope**, select the compartment that contains your target database. Optionally select **Include child compartments** to include target database in the list from child compartments.
3. (Optional) Filter the list of results, under **Filters**, do the following:
   a. (Optional) Select a time period from the **Time period** menu.
   b. (Optional) Select a target database from the **Target database** menu.
4. Click on the name of a target database.
   This will take you to the Configuration details page.
5. Under **Resources**, click **SQL Firewall policies**.
6. Select a SQL Firewall policy from the list.
   This will take you to the Firewall policy details page.
7. Click **Drop**. This will delete the SQL Firewall policy and a SQL Collection will have to be initiated again to re-create this policy.

View and Manage Violations Report

Describes actions that can be take on reports and how to create custom reports.

Modifying Columns in a Violations Report

To add or remove columns in the report, do the following:

1. View a predefined or custom violations report.
2. Click on the **Actions** drop down menu.
3. Click **Manage columns**.
   The Manage columns window is displayed.
4. Select columns that you want displayed in the report.

5. Deselect columns that you want to hide in the report.
6. Click **Save changes**.

Basic Filtering in a Violations Report

To apply basic filters in the report, do the following:

1. View a custom or predefined violations report.
2. Click **Another filter**.
3. Select a filter type, operator, and enter a value. All columns that are available in the report are available as filter types.
4. Click **Apply**.
5. Repeat steps two through four to apply additional filters.

To remove a filter, click the X beside the filter row.

To filter the report based on a total category (for example, Violations blocked), click the total. The list of violations in the table at the bottom of the report is automatically updated. To remove the filter, click the total again.

> **Note:**
>
> Only some totals in your report are single-click filters.

Advanced Filtering in a Violations Report

Advanced filtering of violations can provide flexibility in the way that data is analyzed and reviewed, by allowing organizations to specify complex conditions and multiple criteria that must be met in order for data to be included or excluded from the analysis.

To apply advanced filters in the report, do the following:

1. View a predefined or custom violations report.
2. Click **Show Advanced SCIM Query Builder**.
3. Use the provided filter builder and dropdowns to type in your filter(s). Advanced filtering uses System for Cross-Domain Identity Management (SCIM) syntax and supported operators include:
   - `co`: matches resources with an attribute that contains a given string
   - `eq`: matches resources with an attribute that is equal to a given value (not case sensitive)
   - `eq_cs`: matches resources with an attribute that is equal to a given value (case sensitive)
   - `ew`: matches resources with an attribute that ends with a given string
   - `ge`: matches resources with an attribute that is greater than or equal to a given value
   - `gt`: matches resources with an attribute that is greater than a given value
   - `in`: matches resources with an attribute that is equal to any of given values in list
   - `le`: matches resources with an attribute that is less than or equal to a given value

- `lt`: matches resources with an attribute that is less than a given value
- `ne`: matches resources with an attribute that is not equal to a given value
- `not_in` : matches resources with an attribute that is not equal to any of given values in list
- `pr`: matches resources with an attribute if it has a given value
- `sw`: matches resources with an attribute that starts with a given string

Operators can be grouped using parentheses to specify the order.

Filters can also be combined using logical operators such as `and` and `or`.

> **Note:**
>
> If you have any basic filters currently applied they will appear in the query builder as well.

4. Click **Apply**.

To clear the query builder, click **Clear**. This will clear any basic filters applied as well.

Example 8-1 Context violations and SQL violations that are allowed advanced filter

```
(violationAction eq "ALLOWED")  and ((violationCause eq "context violation")
or (violationCause  eq "SQL violation"))
```

Example 8-2 SQL violations on a specific target database advanced filter

```
(targetName eq "HRApps") and (violationCause eq "SQL violation")
```

Example 8-3 Actions taken on two specific databases since a specifc time advanced filter

```
(operationTime ge "2023-09-11T00:39:43.295Z") and ((targetName eq "HRApps")
or (targetName eq "TF_AUTOMATION"))
```

Tips for Using the Filter Builder to Create Advanced Filters

- Pressing the escape key while in advanced filtering mode will clear the whole query.
- Pressing the space key will display the drop down with the list of available attributes or operators.
- Pressing the space key after entering a value like `targetname (demo_tgt)` will enclose the string with quotes: `("demo_tgt")`.
- Pressing enter will close the drop down listing the operators and attribute names.
- If a value like SQL Firewall policy name has spaces in it, typing space will enclose the first word within quotes, `"policy name"`. You will have to move the cursor back to the enclosed string and continue typing the rest of the string value.
- If you build a filter in advanced filtering that can't be displayed in basic filters, you can't switch back to basic filtering mode. For example, advanced filters with the or condition can't be displayed in basic filtering.

- A custom report with basic filter can be updated with advanced filter and saved.

For more information about SCIM, see the protocol documentation at https://www.rfceditor.org/rfc/rfc7644.

For more information about filtering in SCIM, see the filtering section of the protocol documentation at https://www.rfc-editor.org/rfc/rfc7644#section-3.4.2.2.

Create a Custom Violations Report

You can create a custom report from any violations report, including the predefined AllViolations report. The details saved to the custom reports are those that you are currentlyviewing on screen. You may want to create a custom report if you want to preserve thefilters and columns displayed in a report that you are viewing online. You may alsowant to store your custom reports in specific compartments.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation reports**.
3. Click a report name and modify it as needed. If there aren't any custom reports saved, click the All violations report and make changes to it.
4. Click **Create custom report**.
   The Create custom report dialog box is displayed.
5. Enter a name for your custom report.
6. (Optional) Enter a description for your custom report.
7. Select the compartment to where you want to save your custom report.
8. Click **Create custom report**, and wait for a message that tells you the custom report is created.
9. (Optional) To open and view your custom report, click the **click here** link.
10. (Optional) To return to the report displayed on the screen, click **Close**.

Update a Custom Violations Report

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation reports**.
3. Click **Custom reports** tab.
4. Click a custom report name.
5. Modify the report as needed.
6. Click **Save Report**.
   The custom report is updated.

Delete a Custom Violations Report

When you delete a custom violations report, the report is permanently deleted and cannot berecovered. You cannot delete the predefined All violations report.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation reports**.
3. Click **Custom reports** tab.

4. Click a custom report name.
5. Click **Delete report**.

   A Delete report dialog box is displayed, asking you to confirm the deletion.
6. Click **Delete report**.

Create or Manage a Schedule for a Violations Report

You can create a schedule for a predefined or custom violation report to generate a PDF or XLS report.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resource**, click **Violation reports**.
   The **Violation reports** page is displayed, showing you a list of violation reports.
3. To view a predefined violation report, on the **Predefined reports** tab, in the **Report name** column, click the report name that you want to view.
   The predefined report is displayed.
4. To view a custom violation report, click the **Custom report** tab. In the **Report name** column, click the name of your custom report.
   Your custom report is displayed.
5. Click **Manage report schedule**.
   The **Manage report schedule** panel is displayed, pre-loaded with either the default or modified schedule.
6. (Optional) In the **Schedule report name** box, enter a name for the PDF or XLS report.
7. Select a compartment to store the reports generated by the schedule.
8. For **Report format**, select either a **PDF** or **XLS** output.
9. Select a **Schedule frequency**.
   - If you select weekly, select the day of the week in the **Every** field.
   - If you select monthly, select the day of the month in the **Day** field.
10. In **Time (in UTC)**, select a schedule time.
11. In **Events time span**, select the time span for the violation records.
    For example, selecting Last months and entering 14 pulls violations from the last 14 months from the time the report is run.
12. (Optional) Specify a row limit. If unspecified, the default row limit is 200 rows.
13. Click **Save Schedule**.
    You can access the generated PDF/XLS reports on the **Violation report history** page.

View and Manage Violation Report History

The **Violation report history** page lists all the PDF/XLS violations reports that are automatically generated via a schedule or on-demand by users. On this page, you can view the list of reports generated during the past three months, details about those reports, and download reports. Oracle Data Safe stores these reports for up to three months.

1. Under **Security center**, click **SQL Firewall**.
2. Under **Related resources**, click **Violation report history**.
   The Violation report history table is displayed. It contains the following information:

- **Name** - The name of the violation report
- **State** - Either **Active** or **Updating**, shows if the report is currently accessible or if it is being updated
- **Report definition** - Specifies the name of the report that provides data for this scheduled or generated report
- **Generated time** - The time the report was created
- **Report type** - Generated or Scheduled. Where generated reports are on-demand reports produced outside of the scheduling system and scheduled reports are those produced by the scheduling system
- **File format** - PDF or XLS
- **Download report** - Option to download the report

3. (Optional) Under **Filters**, narrow down the report history page based on the **Report definition**, **Report type**, **File format**, and **Time period**.
4. Click on any report name to see further details including OCID and compartment information.

Create and Modify Event Notifications in SQL Firewall

You can create and modify event notifications in SQL Firewall.

Creating Event Notifications for SQL Firewall

In Data Safe you can create event notifications for SQL Firewall related events. You can use the quickstart template for common events or the advanced event notification workflows to create notifications.

Prerequisites:

Ensure you have the necessary IAM permissions to create event notifications. For more information, see Permissions to Use Contextual Event Notifications in the *Administering Oracle Data Safe* guide.

To create notifications:

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Notifications** tab.
3. Click **Create notification**.
   If you don't have any notifications created for the selected resource then you will see a list of available quickstart templates. You may click on one of these instead.

   The **Create notification** side panel will appear.
4. Select to create an event notification from either a **Quickstart** template or an **Advanced event notification**.
   A Quickstart template allows you to select from a list of common event scenarios. When you create a notification from a quickstart template, the Rule and Event is created automatically.

> **Note:**
>
> The Rule and Event are created in the compartment that you were working in when you started the Notification workflow. Rules and Events will only trigger for the compartment and any child-compartments of the compartment that they were created in.

5. If you selected **Quickstart** in the previous step, make a quickstart **Template selection**. If you selected **Advanced event notification** in the previous step, type in a **Rule name** and select an **Event type**.

   See SQL Firewall Event Types in the *Administering Oracle Data Safe* guide for more information on events.
6. Select to either **Create new topic** or to **Select existing topic**.
7. Select a **Compartment**.

> **Note:**
>
> This compartment is where the topic will be created, not where the rule and event will be monitored in.

8. If you're creating a new topic, type the topic name or, if you're using an existing topic, select the topic name.
9. Select a **Subscription protocol**.
10. Provide the necessary inputs for the selected subscription protocol.
11. Optionally, click **Show Advanced Options** to tag the notification.
    a. Click **+ Another Tag** to create an additional optional tag to organize and track resources in your tenancy.
    b. Select a **Tag Namespace** from the drop-down list.
    c. Provide a **Tag Key** and **Tag Value**.
12. Click **Create notification**.

Modifying Event Notifications For SQL Firewall

After creating event notifications in SQL Firewall in Oracle Data Safe, you can modify the notifications you created.

To modify the event and rule:

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Notifications** tab.
3. Click on an existing event from the **Name** column.

> **Note:**
>
> You will only see the Events that were created directly within Data Safe.

This will bring you to the Rule details page which is part of Oracle Cloud Infrastructure (OCI) Events Service. For more information, see the Events section of the OCI Documentation.

To modify the topic and subscription:

1. Under **Security center**, click **SQL Firewall**.
2. Click the **Notifications** tab.
3. Click on an existing topic from the **Topic** column.

> **Note:**
>
> You will only see the Topics that were created directly within Data Safe.

This will bring you to the Topic Details page which is part of Oracle Cloud Infrastructure (OCI) Notifications. For more information, see the Notifications section of the OCI Documentation.

9

Events

Oracle Cloud Infrastructure Events enables you to create automation based on the state changes of resources throughout your tenancy, including Oracle Data Safe resources.

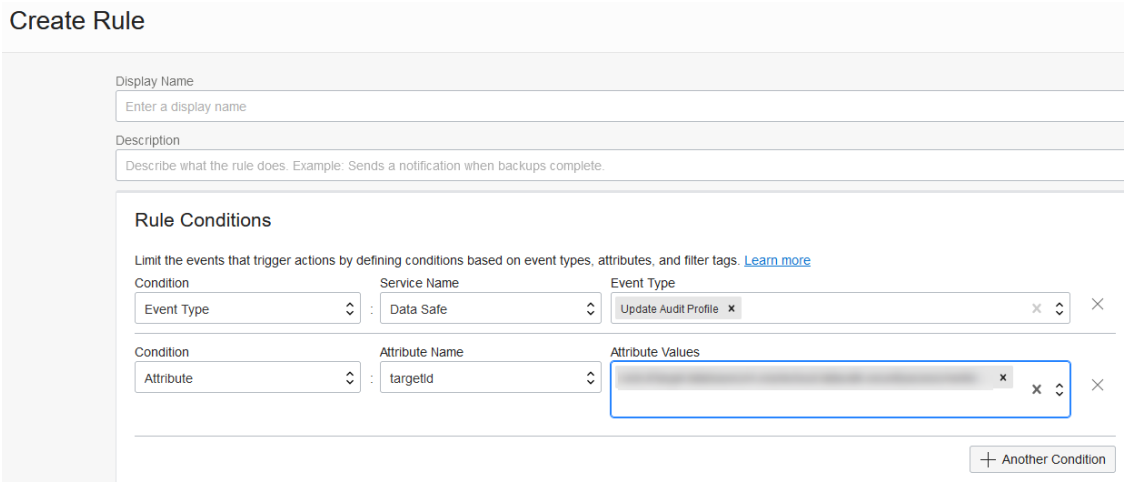
Overview of Oracle Data Safe Events

Administrators can configure the Oracle Data Safe service to emit events in Oracle Cloud Infrastructure, which are structured messages that indicate changes in resources.

Rule Conditions

When you create a rule, you start by configuring a condition. The first condition specifies the event type(s) for which you want to be notified. If you want to set filters on the event types, you can add more conditions that specify attributes and tags.

Let's look at a simple example. Suppose you want to be notified when an audit profile is updated in Oracle Data Safe. To do this, in the event rule, you select the **Update Audit Profile** event type for the first condition. Because you are interested in a particular database, you add a second condition to the rule with a filter on the attribute **targetId**. For its value, you enter the OCID of your target database. Now, if a user updates the audit profile for your target database, you will be notified. The following screenshot shows you the **Create Rule** page in Oracle Cloud Infrastructure with these conditions configured.



Notification Text

Notification text is in JSON format. From the **Create Rule** page in Oracle Cloud Infrastructure, you can preview the text. Simply click the **View example events (JSON)** link and select an

Oracle Data Safe event type. The following is an example for the **Create Audit Archive retrieval - Begin** event type:

```
{
  "eventType": "com.oraclecloud.datasafe.createarchiveretrieval.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T12:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "auditArchiveRetrievals",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
    "additionalDetails": {
      "targetId": "ocid1.datasafetargetdatabase.oc1..unique_ID",
      "startDate": "2021-02-01T00:00:00.000Z",
      "endDate": "2021-05-01T00:00:00.000Z"
    }
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Each event type has its own set of additional details, and some do not have any. In the example above, the `additionalDetails` node shows you target database name, start date, and end date.

About Oracle Data Safe Events

To configure events, you create rules that specify which events can trigger actions. Actions include publishing messages to a stream via the Streaming service, broadcasting a notification message to subscribers via the Notifications service, or invoking functions in Oracle Functions. For example, you can trigger a notification message when a user registers a target database with Oracle Data Safe.

> **Note:**
>
> Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

To learn more about events, see Overview of Events in the Oracle Cloud Infrastructure documentation.

Event Types for Oracle Data Safe

Oracle Data Safe has events types for Security Assessment, User Assessment, Alerts, Activity Auditing, Data Discovery, Data Masking, SQL Firewall, Oracle Data Safe on-premises connectors, Oracle Data Safe private endpoints, and target databases.

Target Database Event Types

The following table describes event types for target databases in Oracle Data Safe.

Friendly Name	Event Type and Description
Create Target Database - Begin	`com.oraclecloud.datasafe.createtargetdatabase.begin` The event type emits when a user creates a target database with Oracle Data Safe.
Create Target Database - End	`com.oraclecloud.datasafe.createtargetdatabase.end` The event type emits when target database creation is completed.
Delete Target Database - Begin	`com.oraclecloud.datasafe.deletetargetdatabase.begin` The event type emits when a user deletes a target database.
Delete Target Database - End	`com.oraclecloud.datasafe.deletetargetdatabase.end` The event type emits when a target database is deleted.
Register Target Database - Begin	`com.oraclecloud.datasafe.registerdatasafetarget.begin` The event type emits when a user registers a target database with Oracle Data Safe.
Register Target Database - End	`com.oraclecloud.datasafe.registerdatasafetarget.end` The event type emits when target database registration is completed.
Deregister Target Database - Begin	`com.oraclecloud.datasafe.deregisterdatasafetarget.begin` The event type emits when a user deregisters a target database with Oracle Data Safe.
Deregister Target Database - End	`com.oraclecloud.datasafe.deregisterdatasafetarget.end` The event type emits when a target deregistration is completed.
Target Database State Change	`com.oraclecloud.datasafe.statechangetargetdatabase` The event type emits when there is a change in a target database's state.
Alert Policy Target Association Patch Begin	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.begin` The event type emits when a user triggers an alert policy target association patch with Oracle Data Safe.
Alert Policy Target Association Patch End	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.end` The event type emits when an alert policy target association patch is completed.
Disabled Target Alert Policy Association	`com.oraclecloud.datasafe.disabledtargetalertpolicyassociation` The event type emits when a target alert policy association is generating more alerts than the threshold permits.

Example 9-1 Notification Text for a Create Target Database - End Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createtargetdatabase.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-02-23T19:15:20.264Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "targetDatabase",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "<availability-domain>"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Create Target Database - End",
  "additionalDetails": [
    {"name": "targetId", "type": "string"},
    {"name": "targetType", "type": "string"}
    ],
  "timeCreated": "2021-02-23T19:15:20.264Z",
  "activationTime": "2021-03-15T00:00:00.000Z"
}
```

Oracle Data Safe On-Premises Connector Event Types

The following table describes event types for Oracle Data Safe on-premises connectors.

Friendly Name	Event Type and Description
Create On-Prem Connector - Begin	`com.oraclecloud.datasafe.createonpremconnector.begin` The event type emits when an Oracle Data Safe on-premises connector creation request is triggered by a user.
Create On-Prem Connector - End	`com.oraclecloud.datasafe.createonpremconnector.end` The event type emits when an on-premises connector creation request is completed.
Delete On-Prem Connector - Begin	`com.oraclecloud.datasafe.deleteonpremconnector.begin` The event type emits when an Oracle Data Safe on-premises connector deletion request is triggered by a user.
Delete On-Prem Connector - End	`com.oraclecloud.datasafe.deleteonpremconnector.end` The event type emits when the on-premises connector deletion request is completed.
On-Prem Connector State Change	`com.oraclecloud.datasafe.statechangeonpremconnector` The event type emits when the state of an Oracle Data Safe on-premises connector changes.

Friendly Name	Event Type and Description
Rotate On-Prem Connector - Begin	`com.oraclecloud.datasafe.updateonpremconnectorwallet.begin` The event type emits when a wallet rotation request for an Oracle Data Safe on-premises connector is triggered by a user.
Rotate On-Prem Connector - End	`com.oraclecloud.datasafe.updateonpremconnectorwallet.end` The event type emits when a wallet rotation request for an Oracle Data Safe on-premises connector is completed.

Example 9-2 Notification Text for the Create On-Prem Connector - Begin Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createonpremconnector.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "onPremConnectors",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
  "serviceName": "Data Safe",
  "displayName": "Create On-Prem Connector - Begin",
  "additionalDetails": [],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Oracle Data Safe Private Endpoint Event Types

The following table describes event types for Oracle Data Safe private endpoints.

Friendly Name	Event Type and Description
Create Private Endpoint - Begin	`com.oraclecloud.datasafe.createdatasafeprivateendpoint.begin` The event type emits when an Oracle Data Safe private endpoint creation request is triggered by a user.
Create Private Endpoint - End	`com.oraclecloud.datasafe.createdatasafeprivateendpoint.end` The event type emits when an Oracle Data Safe private endpoint creation request is completed.

Friendly Name	Event Type and Description
Delete Private Endpoint - Begin	`com.oraclecloud.datasafe.deletedatasafeprivateendpoint.begin` The event type emits when an Oracle Data Safe private endpoint deletion request is triggered by a user.
Delete Private Endpoint - End	`com.oraclecloud.datasafe.deletedatasafeprivateendpoint.end` The event type emits when an Oracle Data Safe private endpoint deletion request is completed.

Example 9-3 Notification Text for the Create Private Endpoint - End Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.createdatasafeprivateendpoint.end",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:07:10.809Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "privateEndpoints",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Create Private Endpoint - End",
  "additionalDetails": [],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Security Assessment Event Types

The following table describes event types for Security Assessment in Oracle Data Safe.

Friendly Name	Event Type and Description
Security Assessment Create Begin	`com.oraclecloud.datasafe.createsecurityassessment.begin` The event type is emitted when a user triggers a security assessment.
Security Assessment Create End	`com.oraclecloud.datasafe.createsecurityassessment.end` The event type is emitted when a security assessment is finished.
Security Assessment Refresh Begin	`com.oraclecloud.datasafe.refreshsecurityassessment.begin` The event type is emitted when a user refreshes a security assessment.

Friendly Name	Event Type and Description
Security Assessment Refresh End	`com.oraclecloud.datasafe.refreshsecurityassessment.end` The event type is emitted when a security assessment is finished refreshing.
Security Assessment Baseline Set Begin	`com.oraclecloud.datasafe.setsecurityassessmentbaseline.begin` The event type is emitted when a user sets a security assessment as a baseline.
Security Assessment Baseline Set End	`com.oraclecloud.datasafe.setsecurityassessmentbaseline.end` The event type is emitted when a set baseline operation on a security assessment is finished.
Security Assessment Baseline Unset Begin	`com.oraclecloud.datasafe.unsetsecurityassessmentbaseline.begin` The event type is emitted when a user unsets a security assessment as a baseline.
Security Assessment Baseline Unset End	`com.oraclecloud.datasafe.unsetsecurityassessmentbaseline.end` The event type is emitted when an unset baseline operation on a security assessment is finished.
Security Assessment Compare Begin	`com.oraclecloud.datasafe.comparesecurityassessment.begin` The event type is emitted when a user compares two security assessments.
Security Assessment Compare End	`com.oraclecloud.datasafe.comparesecurityassessment.end` The event type is emitted when a compare operation for two security assessments is finished.
Security Assessment Drift From Baseline	`com.oraclecloud.datasafe.securityassessmentdriftfrombaseline` The event type is emitted when a security assessment is compared with a baseline assessment and a difference is found.
Security Assessment Report Generate Begin	`com.oraclecloud.datasafe.generatesecurityassessmentreport.begin` The event type is emitted when a user requests to generate a security assessment report.
Security Assessment Report Generate End	`com.oraclecloud.datasafe.generatesecurityassessmentreport.end` The event type is emitted when an operation to generate a security assessment report is finished.
Security Assessment Report Download	`com.oraclecloud.datasafe.downloadsecurityassessmentreport` The event type is emitted when a user requests to download a security assessment report.
Security Assessment Finding Risk Update Begin	`com.oraclecloud.datasafe.updatefinding.begin` The event type is emitted when a user begins changing the risk for a finding.
Security Assessment Finding Risk Update End	`com.oraclecloud.datasafe.updatefinding.end` The event type is emitted when changing the risk for a finding is finished.

> **Note:**
>
> Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

Example 9-4 Notification Text for a Security Assessment Drift From Baseline Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.securityassessmentdriftfrombaseline",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "securityAssessment",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "Security Assessment Drift From Baseline",
  "additionalDetails": [{"name":"targetNames","value":["target1", "target2"]},
{"name":"comparisonId","value": "<baseline_assessment_ID>"} ],
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

User Assessment Event Types

The following table describes event types for User Assessment in Oracle Data Safe.

Friendly Name	Event Type and Description
User Assessment Create Begin	`com.oraclecloud.datasafe.createuserassessment.begin` The event type is emitted when a user triggers a user assessment.
User Assessment Create End	`com.oraclecloud.datasafe.createuserassessment.end` The event type is emitted when a user assessment is finished creating.
User Assessment Refresh Begin	`com.oraclecloud.datasafe.refreshuserassessment.begin` The event type is emitted when a user refreshes a user assessment.

Friendly Name	Event Type and Description
User Assessment Refresh End	com.oraclecloud.datasafe.refreshuserassessment.end The event type is emitted when a user assessment is finished refreshing.
User Assessment Baseline Set Begin	com.oraclecloud.datasafe.setuserassessmentbaseline.begin The event type is emitted when a user sets a user assessment as a baseline assessment.
User Assessment Baseline Set End	com.oraclecloud.datasafe.setuserassessmentbaseline.end The event type is emitted when a set baseline operation on a user assessment is finished.
User Assessment Baseline Unset Begin	com.oraclecloud.datasafe.unsetuserassessmentbaseline.begin The event type is emitted when a user unsets a user assessment as a baseline assessment.
User Assessment Baseline Unset End	com.oraclecloud.datasafe.unsetuserassessmentbaseline.end The event type is emitted when an unset baseline operation on a user assessment is finished.
User Assessment Compare Begin	com.oraclecloud.datasafe.compareuserassessment.begin The event type is emitted when a user compares two user assessments.
User Assessment Compare End	com.oraclecloud.datasafe.compareuserassessment.end The event type is emitted when a compare operation for two user assessments is finished.
User Assessment Drift From Baseline	com.oraclecloud.datasafe.userassessmentdriftfrombaseline The event type is emitted when a user assessment is compared with a baseline and a difference is found.
User Assessment Report Generate Begin	com.oraclecloud.datasafe.generateuserassessmentreport.begin The event type is emitted when a user requests to generate a user assessment report.
User Assessment Report Generate End	com.oraclecloud.datasafe.generateuserassessmentreport.end The event type is emitted when a user assessment report is generated.
User Assessment Report Download	com.oraclecloud.datasafe.downloaduserassessmentreport The event type is emitted when a user requests to download a user assessment report.
Security Policy Report Create Begin	com.oraclecloud.datasafe.createsecuritypolicyreport.begin The event type is emitted when a security policy report is being created.
Security Policy Report Create Complete	com.oraclecloud.datasafe.createsecuritypolicyreport.end The event type is emitted when security policy report creation is completed.
Security Policy Report Delete Begin	com.oraclecloud.datasafe.deletesecuritypolicyreport.begin The event type is emitted when a security policy report is being deleted by the system.

Friendly Name	Event Type and Description
Security Policy Report Delete Complete	`com.oraclecloud.datasafe.deletesecuritypolicyreport.end` The event type is emitted when a security policy report deletion is completed.
Security Policy Report Refresh Begin	`com.oraclecloud.datasafe.refreshsecuritypolicyreport.begin` The event type is emitted when a security policy report is being refreshed.
Security Policy Report Refresh Complete	`com.oraclecloud.datasafe.refreshsecuritypolicyreport.end` The event type is emitted when a security policy report is refreshed.
User Assessment Password Expiry Date	`com.oraclecloud.datasafe.userassessmentpasswordexpirydate` This event is triggered twice: first when the user has fewer than 90 days remaining until password expiration, and again when fewer than 30 days remain.

Note:

Any Oracle Data Safe event for User Assessment or Security Assessment that you created in the past that uses an old event type name, for example, `com.oraclecloud.datasafe.securityassessmentrefresh.begin`, needs to be dropped and recreated so that it uses the new friendly name, for example, `Security Assessment Refresh Begin`; otherwise, the event will not work.

Example 9-5 Notification Text for a User Assessment Drift From Baseline Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.userassessmentdriftfrombaseline",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-10T22:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "userAssessment",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1"
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  },
  "serviceName": "Data Safe",
  "displayName": "User Assessment Drift From Baseline",
  "additionalDetails": [{"name":"targetNames","value":["target1", "target2"]},
{"name":"comparisonId","value": "<baseline_assessment_ID>"} ],
```

```
  "timeCreated": "2020-09-10T22:06:48.011Z"
}
```

Activity Auditing Event Types

The following table describes event types for Activity Auditing in Oracle Data Safe.

Friendly Name	Event Type and Description
Audit Archive Retrieval Create Begin	`com.oraclecloud.datasafe.createarchiveretrieval.begin` An event is emitted when an archive retrieval is started.
Audit Archive Retrieval Create End	`com.oraclecloud.datasafe.createarchiveretrieval.end` An event is emitted when an archive retrieval is finished.
Audit Archive Retrieval Delete Begin	`com.oraclecloud.datasafe.deletearchiveretrieval.begin` An event is emitted when an archive retrieval delete is started.
Audit Archive Retrieval Delete End	`com.oraclecloud.datasafe.deletearchiveretrieval.end` An event is emitted when an archive retrieval delete is finished.
Audit Events Post Retention Purge	`com.oraclecloud.datasafe.purgeretention` An event is emitted when the retention period for audit records is reached and the audit events are being deleted from Data Safe.
Audit Policy Provision Begin	`com.oraclecloud.datasafe.provisionauditpolicy.begin` An event is emitted when an audit policy provisioning is started.
Audit Policy Provision End	`com.oraclecloud.datasafe.provisionauditpolicy.end` An event is emitted when an audit policy provisioning ends.
Audit Profile Retention Update Begin	`com.oraclecloud.datasafe.changeretention.begin` An event is emitted when an audit retention update is started. Example, when online/offline audit data retention settings are being updated.
Audit Profile Retention Update End	`com.oraclecloud.datasafe.changeretention.end` An event is emitted when an audit retention update is completed. Example, when online/offline audit data retention settings are successfully updated.
Audit Policy Retrieve Begin	`com.oraclecloud.datasafe.retrieveauditpolicies.begin` An event is emitted when an audit policy retrieval is started.
Audit Policy Retrieve End	`com.oraclecloud.datasafe.retrieveauditpolicies.end` An event is emitted when an audit policy retrieval is finished.
Audit Profile Update Begin	`com.oraclecloud.datasafe.updateauditprofile.begin` An event is emitted when an audit profile update is started.
Audit Profile Update End	`com.oraclecloud.datasafe.updateauditprofile.end` An event is emitted when an audit profile update is completed.
Audit Trail Collection Free Limit Warning	`com.oraclecloud.datasafe.auditcollectionwarning` An event is emitted when an audit collection reaches 80% of the free limit.
Audit Trail Resume Begin	`com.oraclecloud.datasafe.resumeaudittrail.begin` An event is emitted when an audit trail resume begins.
Audit Trail Resume End	`com.oraclecloud.datasafe.resumeaudittrail.end` An event is emitted when an audit trail resume ends.

Friendly Name	Event Type and Description
Audit Trail Start Begin	com.oraclecloud.datasafe.startauditrail.begin An event is emitted when an audit trail start begins.
Audit Trail Start End	com.oraclecloud.datasafe.startauditrail.end An event is emitted when an audit trail start ends.
Audit Trail Stop Begin	com.oraclecloud.datasafe.stopauditrail.begin An event is emitted when an audit trail stop begins.
Audit Trail Stop End	com.oraclecloud.datasafe.stopauditrail.end An event is emitted when an audit trail is stopped automatically or manually.
Audit Trail Update Begin	com.oraclecloud.datasafe.updateauditrail.begin An event is emitted when audit trail update is started.
Audit Trail Update End	com.oraclecloud.datasafe.updateauditrail.end An event is emitted when audit trail update is finished.
Report Generate Begin	com.oraclecloud.datasafe.generatereport.begin An event is emitted when a report generation is started.
Report Generate End	com.oraclecloud.datasafe.generatereport.end An event is emitted when a report generation is completed.
Report Schedule Begin	com.oraclecloud.datasafe.schedulereport.begin An event is emitted when a new report schedule is being created.
Report Schedule End	com.oraclecloud.datasafe.schedulereport.end An event is emitted when a new report schedule is created successfully.
Report Schedule Delete Begin	com.oraclecloud.datasafe.removeschedulereport.begin An event is emitted when report schedule delete is started.
Report Schedule Delete End	com.oraclecloud.datasafe.removeschedulereport.end An event is emitted when report schedule delete is completed.
Scheduled Report Generated	com.oraclecloud.datasafe.scheduledreportcomplete An event is emitted when a scheduled report is generated successfully.

Example 9-6 Notification text for the event type Audit Policy Provision Begin

```
{
  "eventType": "com.oraclecloud.datasafe.provisionauditpolicy.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "auditPolicies",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
    "additionalDetails": {
      "targetId": "ocid1.datasafetargetdatabase.oc1..unique_ID"
    }
```

```
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Alert Event Types

The following table describes event types for alerts in Oracle Data Safe.

Friendly Name	Event Type and Description
Alert Generated	`com.oraclecloud.datasafe.generateauditalert` An event is emitted when an audit alert is generated.
Alert Generation Throttled	`com.oraclecloud.datasafe.throttlealertgeneration` An event is emitted when alert generation has been temporarily disabled for the alert policy because it generated more alerts than the threshold of 1,000 per ten minutes.
Alert Policy Target Association Patch Begin	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.begin` An event is emitted when target alert policy associations are created or updated.
Alert Policy Target Association Patch End	`com.oraclecloud.datasafe.patchtargetalertpolicyassociation.end` An event is emitted when target alert policy associations updates have completed.
Alert UpdateAll Begin	`com.oraclecloud.datasafe.alertsupdate.begin` An event is emitted when Alert updateAll is started.
Alert UpdateAll End	`com.oraclecloud.datasafe.alertsupdate.end` An event is emitted when Alert updateAll is completed.
Create Alert Policy Begin	`com.oraclecloud.datasafe.createalertpolicy.begin` An event is emitted when creation of a custom alert policy is started.
Create Alert Policy End	`com.oraclecloud.datasafe.createalertpolicy.end` An event is emitted when creation of a custom alert policy is finished.
Create Alert Policy Rule Begin	`com.oraclecloud.datasafe.createalertpolicyrule.begin` An event is emitted when creation of a custom alert policy rule is started.
Create Alert Policy Rule End	`com.oraclecloud.datasafe.createalertpolicyrule.end` An event is emitted when creation of a custom alert policy rule is finished.
Delete Alert Policy Begin	`com.oraclecloud.datasafe.deletealertpolicy.begin` An event is emitted when deletion of a custom alert policy is started.
Delete Alert Policy End	`com.oraclecloud.datasafe.deletealertpolicy.end` An event is emitted when deletion of a custom alert policy is finished.
Delete Alert Policy Rule Begin	`com.oraclecloud.datasafe.deletealertpolicyrule.begin` An event is emitted when deletion of a custom alert policy rule is started.

Friendly Name	Event Type and Description
Delete Alert Policy Rule End	com.oraclecloud.datasafe.deletealertpolicyrule.end An event is emitted when deletion of a custom alert policy rule is finished.
Update Alert Policy Begin	com.oraclecloud.datasafe.updatealertpolicy.begin An event is emitted when a custom alert policy update is started.
Update Alert Policy End	com.oraclecloud.datasafe.updatealertpolicy.end An event is emitted when a custom alert policy update is finished.
Update Alert Policy Rule Begin	com.oraclecloud.datasafe.updatealertpolicyrule.begin An event is emitted when a custom alert policy rule update is started.
Update Alert Policy Rule End	com.oraclecloud.datasafe.updatealertpolicyrule.end An event is emitted when a custom alert policy rule update is finished.

Example 9-7 Notification Text for an Audit Alert Generated Event Type

```
{
  "eventType": "com.oraclecloud.datasafe.generateauditalert",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2020-09-29T16:03:41.293Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.compartment.oc1..unique_ID",
    "compartmentName": "example_compartment",
    "resourceName": "alerts",
    "resourceId": "ocid1.datasafealert.oc1.phx.unique_ID",
    "availabilityDomain": "availability_domain",
    "additionalDetails": {
      "status": "OPEN",
      "displayName": "Failed logon by Admin user",
      "description": "Failed logon by Admin user was detected",
      "severity": "HIGH",
      "targetId": "ocid1.datasafetarget.oc1.phx.unique_ID",
      "targetName": "target_sa",
      "policyId": "ocid1.datasafealertpolicy.oc1.iad.unique_ID",
      "timeCreated": "2020-09-29T16:03:31.293Z",
      "timeUpdated": "2020-09-29T16:03:42.736Z",
      "osUserName": "dscs",
      "operationTime": "2020-09-29T15:29:51.404Z",
      "operation": "Login on target database",
      "operationStatus": "Success",
      "clientHostname": "jobsvm3002.jobsvm.stestvcn.oraclevcn.com",
      "clientIPs": "10.0.4.15,10.0.4.16,10.0.4.14",
      "clientId": "ORACLE$_DATA_SAFE#",
      "clientProgram": "JDBC Thin Client",
      "userName": "user1",
      "objectType": "UNIFIED_AUDIT_TRAIL",
      "commandText": "SELECT * FROM AUDSYS.UNIFIED_AUDIT_TRAIL WHERE
\"EVENT_TIMESTAMP\"<=:1 AND \"EVENT_TIMESTAMP\">:2 \u0000",
      "commandParam": " #1(31):02-JUL-21 12.42.15.044000000 PM #2(31):02-
```

```
JUL-21 12.34.22.509000000 PM"
    }
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.compartment.oc1..unique_ID"
  }
}
```

Data Discovery Event Types

The following table describes event types for Data Discovery in Oracle Data Safe.

Friendly Name	Event Type and Description
Create Sensitive Type Group Begin	`com.oraclecloud.datasafe.createsensitivetypegroup.begin` The event type emits when a sensitive type group creation request is triggered.
Create Sensitive Type Group End	`com.oraclecloud.datasafe.createsensitivetypegroup.end` The event type emits when a sensitive type group creation request is completed
Delete Sensitive Type Group Begin	`com.oraclecloud.datasafe.deletesensitivetypegroup.begin` The event type emits when a sensitive type group delete request is triggered.
Delete Sensitive Type Group End	`com.oraclecloud.datasafe.deletesensitivetypegroup.end` The event type emits when a sensitive type group delete request is completed.
Patch Grouped Sensitive Types Begin	`com.oraclecloud.datasafe.patchgroupedsensitivetypes.begin` The event type emits when the request for a sensitive type to be added to or to be removed from a sensitive type group is triggered.
Patch Grouped Sensitive Types End	`com.oraclecloud.datasafe.patchgroupedsensitivetypes.end` The event type emits when the request for a sensitive type to be added to or to be removed from a sensitive type group is completed.
Referential Relations Create Begin	`com.oraclecloud.datasafe.CreateReferentialRelation.begin` The event type emits when a referential relation creation request in a sensitive data model is triggered.
Referential Relations Create End	`com.oraclecloud.datasafe.CreateReferentialRelation.end` The event type emits when a referential relation creation request in a sensitive data model is completed.
Referential Relations Delete Begin	`com.oraclecloud.datasafe.DeleteReferentialRelation.begin` The event type emits when a referential relation deletion request in a sensitive data model is triggered.
Referential Relations Delete End	`com.oraclecloud.datasafe.DeleteReferentialRelation.end` The event type emits when a referential relation deletion request in a sensitive data model is completed.
Sensitive Column Create Begin	`com.oraclecloud.datasafe.createsensitivecolumn.begin` The event type emits when a sensitive column creation request is triggered.

Friendly Name	Event Type and Description
Sensitive Column Create End	`com.oraclecloud.datasafe.createsensitivecolumn.end` The event type emits when a sensitive column creation request is completed.
Sensitive Column Delete Begin	`com.oraclecloud.datasafe.deletesensitivecolumn.begin` The event type emits when a sensitive column delete request is triggered.
Sensitive Column Delete End	`com.oraclecloud.datasafe.deletesensitivecolumn.end` The event type emits when a sensitive column delete request is completed.
Sensitive Data Model Create Begin	`com.oraclecloud.datasafe.createsensitivedatamodel.begin` The event type emits when a sensitive data model creation request is triggered.
Sensitive Data Model Create End	`com.oraclecloud.datasafe.createsensitivedatamodel.end` The event type emits when a sensitive data model creation request is completed.
Sensitive Data Model Delete Begin	`com.oraclecloud.datasafe.deletesensitivedatamodel.begin` The event type emits when a sensitive data model deletion request is triggered.
Sensitive Data Model Delete End	`com.oraclecloud.datasafe.deletesensitivedatamodel.end` The event type emits when a sensitive data model deletion request is triggered.
Sensitive Data Model Update Begin	`com.oraclecloud.datasafe.updatesensitivedatamodel.begin` The event type emits when a sensitive data model update request is triggered.
Sensitive Data Model Update End	`com.oraclecloud.datasafe.updatesensitivedatamodel.end` The event type emits when a sensitive data model update request is completed.
Sensitive Discovery Job Create Begin	`com.oraclecloud.datasafe.creatediscoveryjob.begin` The event type emits when an incremental discovery job creation request is triggered.
Sensitive Discovery Job Create End	`com.oraclecloud.datasafe.creatediscoveryjob.end` The event type emits when an incremental discovery job creation request is completed.
Sensitive Type Create Begin	`com.oraclecloud.datasafe.createsensitivetype.begin` The event type emits when a sensitive type request is triggered.
Sensitive Type Create End	`com.oraclecloud.datasafe.createsensitivetype.end` The event type emits when a sensitive type creation request is completed.
Sensitive Type Delete	`com.oraclecloud.datasafe.deletesensitivetype` The event type emits when a sensitive type delete request is completed.
Sensitive Types Export Create Begin	`com.oraclecloud.datasafe.createsensitivetypesexport.begin` The event type is emitted when a sensitive types export resource creation request is triggered.

Friendly Name	Event Type and Description
Sensitive Types Export Create End	com.oraclecloud.datasafe.createsensitivetypesexport.end The event type emits when a sensitive types export resource creation request is completed.
Sensitive Types Export Update Begin	com.oraclecloud.datasafe.updatesensitivetypesexport.begin The event type is emitted when a sensitive types export resource update request is triggered.
Sensitive Types Export Update End	com.oraclecloud.datasafe.updatesensitivetypesexport.end The event type is emitted when a sensitive types export resource update request is completed.
Sensitive Type Update Begin	com.oraclecloud.datasafe.updatesensitivetype.begin The event type emits when a sensitive type update request is triggered.
Sensitive Type Update End	com.oraclecloud.datasafe.updatesensitivetype.end The event type emits when a sensitive type update request is completed.
Update Sensitive Type Group Begin	com.oraclecloud.datasafe.updatesensitivetypegroup.begin The event type emits when a sensitive type group update request is triggered.
Update Sensitive Type Group End	com.oraclecloud.datasafe.updatesensitivetypegroup.end The event type emits when a sensitive type group update request is completed.

Example 9-8 Notification text for the event type Sensitive Type Create Begin

```
{
  "eventType": "com.oraclecloud.datasafe.createsensitivetype.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "sensitiveTypes",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

Data Masking Event Types

The following table describes event types for Data Masking in Oracle Data Safe.

Friendly Name	Event Type and Description
Masking Column Delete	`com.oraclecloud.datasafe.deletemaskingcolumn` The event type emits when a masking column delete request is completed.
Masking Columns Patch Begin	`com.oraclecloud.datasafe.patchmaskingcolumns.begin` The event type emits when a masking columns patch request is triggered by a user.
Masking Columns Patch End	`com.oraclecloud.datasafe.patchmaskingcolumns.end` The event type emits when a masking columns patch request is completed.
Masking Health Check Begin	`com.oraclecloud.datasafe.generatehealthreport.begin` The event type emits when a masking policy health report creation request is triggered by a user.
Masking Health Check Delete Begin	`com.oraclecloud.datasafe.deletemaskingpolicyhealthreport.begin` The event type emits when a masking policy health report deletion request is triggered by a user.
Masking Health Check Delete End	`com.oraclecloud.datasafe.deletemaskingpolicyhealthreport.end` The event type emits when a masking policy health report deletion request is completed.
Masking Health Check End	`com.oraclecloud.datasafe.generatehealthreport.end` The event type emits when a masking policy health report creation request is completed.
Masking Job Begin	`com.oraclecloud.datasafe.mask.begin` The event type emits when a masking job creation request is triggered by a user.
Masking Job End	`com.oraclecloud.datasafe.mask.end` The event type emits when a masking job creation request is completed.
Masking Library Format Create Begin	`com.oraclecloud.datasafe.createlibrarymaskingformat.begin` The event type emits when a library masking format creation request is triggered by a user.
Masking Library Format Create End	`com.oraclecloud.datasafe.createlibrarymaskingformat.end` The event type emits when a library masking format creation request is completed.
Masking Library Format Delete	`com.oraclecloud.datasafe.deletelibrarymaskingformat` The event type emits when a library masking format delete request is completed.
Masking Library Format Update Begin	`com.oraclecloud.datasafe.updatelibrarymaskingformat.begin` The event type emits when a library masking format update request is triggered by a user.
Masking Library Format Update End	`com.oraclecloud.datasafe.updatelibrarymaskingformat.end` The event type emits when a library masking format update request is completed.

Friendly Name	Event Type and Description
Masking Policy Create Begin	com.oraclecloud.datasafe.createmaskingpolicy.begin The event type emits when a masking policy creation request is triggered by a user.
Masking Policy Create End	com.oraclecloud.datasafe.createmaskingpolicy.end The event type emits when a masking policy creation request is completed.
Masking Policy Delete Begin	com.oraclecloud.datasafe.deletemaskingpolicy.begin The event type emits when a masking policy deletion request is triggered by a user.
Masking Policy Delete End	com.oraclecloud.datasafe.deletemaskingpolicy.end The event type emits when a masking policy deletion request is completed.
Masking Policy Update Begin	com.oraclecloud.datasafe.updatemaskingpolicy.begin The event type emits when a masking policy update request is triggered by a user.
Masking Policy Update End	com.oraclecloud.datasafe.updatemaskingpolicy.end The event type emits when a masking policy update request is completed.
Masking Report Delete Begin	com.oraclecloud.datasafe.deletemaskingreport.begin The event type emits when a masking report delete request is triggered by a user.
Masking Report Delete End	com.oraclecloud.datasafe.deletemaskingreport.end The event type emits when a masking report delete request is completed.

Example 9-9 Notification text for the event type Masking Library Format Create Begin

```
{
  "eventType": "com.oraclecloud.datasafe.createlibrarymaskingformat.begin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "DataSafe",
  "eventTime": "2021-11-18T11:06:46.588Z",
  "contentType": "application/json",
  "data": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID",
    "compartmentName": "example-compartment",
    "resourceName": "libraryMaskingFormats",
    "resourceId": "ocid1.coreservicesworkrequest.oc1..unique_ID",
    "availabilityDomain": "ad1",
  },
  "eventID": "unique_ID",
  "extensions": {
    "compartmentId": "ocid1.tenancy.oc1..unique_ID"
  }
}
```

SQL Firewall Event Types

The following table describes event types for SQL Firewall in Oracle Data Safe.

Friendly Name	Event Type and Description
Database Security Config Cleanup	`com.oraclecloud.datasafe.cleanupdatabasesecurityconfig` The event is emitted when a database security configuration is deleted.
Database Security Config Create Begin	`com.oraclecloud.datasafe.createdatabasesecurityconfig.begin` The event is emitted when a database security configuration is started.
Database Security Config Create End	`com.oraclecloud.datasafe.createdatabasesecurityconfig.end` The event is emitted when a database security configuration is finished.
Database Security Config Refresh Begin	`com.oraclecloud.datasafe.refreshdatabasesecurityconfig.begin` The event is emitted when a database security configuration refresh is started.
Database Security Config Refresh End	`com.oraclecloud.datasafe.refreshdatabasesecurityconfig.end` The event is emitted when a database security configuration refresh is finished.
Database Security Config Update Begin	`com.oraclecloud.datasafe.updatedatabasesecurityconfig.begin` The event is emitted when a database security configuration update is started.
Database Security Config Update End	`com.oraclecloud.datasafe.updatedatabasesecurityconfig.end` The event is emitted when a database security configuration update is finished.
Security Policy Auto Create	`com.oraclecloud.datasafe.autocreatesecuritypolicy` The event is emitted when a security policy is created by the system.
Security Policy Cleanup	`com.oraclecloud.datasafe.cleanupsecuritypolicy` The event is emitted when a security policy is deleted by the system.
Security Policy Deployment Auto Create	`com.oraclecloud.datasafe.autocreatesecuritydeploymentpolicy` The event is emitted when a security policy deployment is created by the system.
Security Policy Deployment Cleanup	`com.oraclecloud.datasafe.cleanupsecuritydeploymentpolicy` The event is emitted when a security policy deployment is deleted.
Security Policy Deployment Update Begin	`com.oraclecloud.datasafe.updatesecuritydeploymentpolicy.begin` This event is emitted when a security policy deployment update is started.
Security Policy Deployment Update End	`com.oraclecloud.datasafe.updatesecuritydeploymentpolicy.end` This event is emitted when a security policy deployment update is finished.
Security Policy Update Begin	`com.oraclecloud.datasafe.updatesecuritypolicy.begin` The event is emitted when a security policy update is started.

Friendly Name	Event Type and Description
Security Policy Update End	com.oraclecloud.datasafe.updatesecuritypolicy.end This event is emitted when a security policy update is finished.
SQL Firewall Allowed SQL Bulk Create Begin	com.oraclecloud.datasafe.BulkCreateSqlFirewallAllowedSqls.begin The event is emitted when a bulk create of allowed SQLs is started.
SQL Firewall Allowed SQL Bulk Create End	com.oraclecloud.datasafe.BulkCreateSqlFirewallAllowedSqls.end The event is emitted when a bulk create of allowed SQLs is finished.
SQL Firewall Allowed SQL Bulk Delete Begin	com.oraclecloud.datasafe.BulkDeleteSqlFirewallAllowedSqls.begin This event is emitted when a bulk delete of allowed SQLs is started.
SQL Firewall Allowed SQL Bulk Delete End	com.oraclecloud.datasafe.BulkDeleteSqlFirewallAllowedSqls.end This event is emitted when a bulk delete of allowed SQLs is finished.
SQL Firewall Allowed SQL Delete Begin	com.oraclecloud.datasafe.DeleteSqlFirewallAllowedSql.begin This event is emitted when a delete of allowed SQL is started.
SQL Firewall Allowed SQL Delete End	com.oraclecloud.datasafe.DeleteSqlFirewallAllowedSql.end This event is emitted when a delete of allowed SQL is finished.
SQL Firewall Collection Auto Create	com.oraclecloud.datasafe.autocreatesqlcollection The event is emitted when a SQL Firewall collection is created by the system.
SQL Firewall Collection Cleanup	com.oraclecloud.datasafe.cleanupsqlcollection The event is emitted when a SQL Firewall collection is deleted by the system.
SQL Firewall Collection Create Begin	com.oraclecloud.datasafe.createsqlcollection.begin The event is emitted when creation of a SQL Firewall collection is started.
SQL Firewall Collection Create End	com.oraclecloud.datasafe.createsqlcollection.end The event is emitted when creation of a SQL Firewall collection is finished.
SQL Firewall Collection Delete Begin	com.oraclecloud.datasafe.deletesqlcollection.begin The event is emitted when deletion of a SQL Firewall collection is started.
SQL Firewall Collection Delete End	com.oraclecloud.datasafe.deletesqlcollection.end The event is emitted when deletion of a SQL Firewall collection is finished.
SQL Firewall Collection Insights Refresh Begin	com.oraclecloud.datasafe.refreshsqlcollectionloginsights.begin The event is emitted when a SQL Firewall collection insights refresh is started.
SQL Firewall Collection Insights Refresh End	com.oraclecloud.datasafe.refreshsqlcollectionloginsights.end The event is emitted when a SQL Firewall collection insights refresh is finished.
SQL Firewall Collection Logs Purge Begin	com.oraclecloud.datasafe.purgesqlcollectionlogs.begin The event is emitted when a SQL Firewall collection logs purge is started.

Friendly Name	Event Type and Description
SQL Firewall Collection Logs Purge End	`com.oraclecloud.datasafe.purgesqlcollectionlogs.end` The event is emitted when a SQL Firewall collection logs purge is finished.
SQL Firewall Collection Start Begin	`com.oraclecloud.datasafe.startsqlcollection.begin` The event is emitted when a SQL Firewall collection is started.
SQL Firewall Collection Start End	`com.oraclecloud.datasafe.startsqlcollection.end` The event is emitted when a SQL Firewall collection is finished.
SQL Firewall Collection Stop Begin	`com.oraclecloud.datasafe.stopsqlcollection.begin` The event is emitted when a SQL Firewall collection stop is started.
SQL Firewall Collection Stop End	`com.oraclecloud.datasafe.stopsqlcollection.end` The event is emitted when a SQL Firewall collection stop is finished.
SQL Firewall Collection Update Begin	`com.oraclecloud.datasafe.updatesqlcollection.begin` This event is emitted when a SQL firewall collection update is started.
SQL Firewall Collection Update End	`com.oraclecloud.datasafe.updatesqlcollection.end` This event is emitted when a SQL Firewall collection update is finished.
SQL Firewall Policy Auto Create	`com.oraclecloud.datasafe.autocreatesqlfirewallpolicy` The event is emitted when a SQL Firewall policy is created by a system.
SQL Firewall Policy Cleanup	`com.oraclecloud.datasafe.cleanupsqlfirewallpolicy` The event is emitted when a SQL Firewall policy is deleted.
SQL Firewall Policy Delete Begin	`com.oraclecloud.datasafe.deletesqlfirewallpolicy.begin` The event is emitted when deletion for a SQL Firewall policy is started.
SQL Firewall Policy Delete End	`com.oraclecloud.datasafe.deletesqlfirewallpolicy.end` The event is emitted when deletion for a SQL Firewall policy is finished.
SQL Firewall Policy Generate Begin	`com.oraclecloud.datasafe.generatesqlfirewallpolicy.begin` The event is emitted when generation of a SQL Firewall policy is started.
SQL Firewall Policy Generate End	`com.oraclecloud.datasafe.generatesqlfirewallpolicy.end` The event is emitted when generation of a SQL Firewall policy is finished.
SQL Firewall Policy Update Begin	`com.oraclecloud.datasafe.updatesqlfirewallpolicy.begin` This event is emitted when a SQL Firewall policy update is started.
SQL Firewall Policy Update End	`com.oraclecloud.datasafe.updatesqlfirewallpolicy.end` This event is emitted when a SQL Firewall policy update is finished.

Event Notifications in Data Safe

Instead of working in OCI Events and Notifications to create rules and subscribe to topics, Data Safe allows you to create event notifications and subscriptions directly. This allows you to remain in the context of Data Safe while creating and modifying notifications for OCI Events.

Through the **Notifications** tab available in Data Safe's features, you can create OCI Event notifications using predefined templates or an advanced set up. In one simple workflow you create the event, rule, topic, and subscription necessary to receive OCI Event notifications. In addition, you can set up Alarm notifications for Alerts which can be configured to notify you if a specific trigger happens a set number of times in a specified time frame.

The simplified notification workflow allows you to focus on the available events for the feature that you're working within and retain the context of your specific resources. For example, if you'd like to be notified whenever a masking job is completed, you can create that notification

directly within Data masking. The notifications workflow is available within all of Data Safe's features and you can find more specific information in the below topics:

- Create and Modify Event Notifications for Targets and Connectivity Options
- Create and Modify Event Notifications in Security Assessment
- Create and Modify Event Notifications in User Assessment
- Create and Modify Event Notifications in Activity Auditing
- Create and Modify Event and Alarm Notifications in Alerts
- Create and Modify Event Notifications in Data Discovery
- Create and Modify Event Notifications in Data Masking
- Create and Modify Event Notifications in SQL Firewall

Related Topics

- OCI Events
- OCI Notifications
- OCI Monitoring

10

Reference

This section contains reference materials.

Regular Expressions

You can use regular expressions to describe a set of strings based on common characteristics shared by each string in the set.

A regular expression is basically a sequence of characters that defines a search pattern, which is used for pattern matching. Regular expressions vary in complexity, but once you understand the basics of how they are constructed, you can decipher or create any regular expression.

String Literals

The most basic form of pattern matching is the match of a string literal. For example, if the regular expression is `EMP` and the input string is `EMP`, the match succeeds because the strings are identical. This regular expression also matches any string containing `EMP`, such as `EMPLOYEE`, `TEMP`, and `TEMPERATURE`.

Metacharacters

You can also use some special characters that affect the way a pattern is matched. One of the most common ones is the dot (`.`) symbol, which matches any character. For example, `EMPLOYEE.ID` matches `EMPLOYEE_ID` and `EMPLOYEE-ID`, but not `EMPLOYEE_VERIFICATION_ID`. Here, the dot is a metacharacter — a character with special meaning interpreted by the matcher.

Some other metacharacters are: `^ $ ? + * \ - [ ] ( ) { }`.

If you want a metacharacter to be treated literally (as an ordinary character), you can use a backslash (`\`) to escape it. For example, the regular expression `9\+9` matches `9+9`.

Character Classes

A character class is a set of characters enclosed within square brackets. It specifies the characters that successfully match a single character from a given input string.

The following table describes some common regular expression constructs.

Construct	Description
`[abc]`	Matches one of the characters mentioned within square brackets. Example: `EMPLOYE[ER]` matches `EMPLOYEE` and `EMPLOYER`.
`[^abc]`	Matches any character except the ones mentioned within square brackets. Example: `[^BC]AT` matches `RAT` and `HAT`, but does not match `BAT` and `CAT`.

Construct	Description
`[A-Z0-9]`	Matches any character in the range mentioned within square brackets. To specify a range, simply insert the dash metacharacter "-" between the first and last character to be matched; for example, `[1-5]` or `[A-M]`. You can also place different ranges beside each other within the class to further expand the match possibilities. Example: `[B-F]AT` matches `BAT`, `CAT`, `DAT`, `EAT`, and `FAT`, but does not match `AAT` and `GAT`.

Oracle Data Safe also supports predefined character classes.

Capturing Groups

You can use capturing groups to treat multiple characters as a single unit. A capturing group is created by placing the characters to be grouped inside a set of parentheses. For example, the regular expression `(SSN)` creates a single group containing the letters `S`, `S`, and `N`.

Quantifiers

You can use quantifiers to specify the number of occurrences to match against.

The following table describes some common quantifiers.

Quantifier	Description
`X?`	Matches zero or one occurrence of the specified character or group of characters. Example: `SSN_NUMBERS?` matches strings `SSN_NUMBER` and `SSN_NUMBERS`.
`X*`	Matches zero or more occurrences of the specified character or group of characters. Example: `TERM.*DATE` matches strings like `TERMDATE`, `TERM_DATE` and `LAST_TERMINATION_DATE`.
`X+`	Matches one or more occurrences of the specified character or group of characters. Example: `TERM.+DATE` matches strings like `TERM_DATE` and `TERMINATION_DATE`, but not `TERMDATE`.
`X{n}`	Matches the specified character or group of characters exactly `n` times. Example: `9{3}` matches `999`, but not `99`.
`X{n,}`	Matches the specified character or group of characters at least `n` times. Example: `9{3,}` matches `999`, `9999`, and `99999`, but not `99`.
`X{n,m}`	Matches the specified character or group of characters at least `n` times but not more than m times. Example: `9{3,4}` matches `999` and `9999`, but not `99`.

You can also use quantifiers with character classes and capturing groups.

An example of regular expression using character class is `SSN[0-9]+`, which matches strings like `SSN0`, `SSN1`, and `SSN12`. Here, `[0-9]` is a character class and is allowed one or more times. The regular expression does not match `SSN`.

An example of regular expression using capturing group is `SSN_NUM(BER)?`, which matches `SSN_NUM` and `SSN_NUMBER`. `(BER)` is a capturing group and is allowed zero or one time.

Boundary Matchers

You can use boundary matchers to make pattern matching more precise by specifying where in the string the match should take place. For example, you might be interested in finding a particular word, but only if it appears at the beginning or end of an input string.

The following table describes common boundary matchers.

Boundary Construct	Description
`^`	Matches the specified character or group of characters at the beginning of a string (starts with search). Example: `^VISA` matches strings beginning with `VISA`.
`$`	Matches the specified character or group of characters at the end of a string (ends with search). Example: `NUMBER$` matches strings ending with `NUMBER`.
`\b`	Marks a word boundary. Matches the character or group of characters specified between a pair of `\b` only if it is a separate word (as opposed to substring within a longer string). Example: `\bAGE\b` matches strings like `EMPLOYEE AGE` and `PATIENT AGE INFORMATION`, but does not match strings like `AGEING` and `EMPLOYEEAGE`.

If no boundary matcher is specified, a contains search is performed. For example, `ELECTORAL` matches strings containing `ELECTORAL`, such as `ELECTORAL_ID`, `ID_ELECTORAL`, and `ELECTORALID`.

An exact match search can be performed by using `^` and `$` together. For example, `^ADDRESS$` searches for the exact string `ADDRESS`. It matches the string `ADDRESS`, but does not match strings like `PRIMARY_ADDRESS` and `ADDRESS_HOME`.

Logical Operators

If you want to match any one of the characters or group of characters separated by pipe, you can use the pipe or vertical bar character (`|`) . For example, `EMPLOY(EE|ER)_ID` matches `EMPLOYEE_ID` and `EMPLOYER_ID`.

Examples

`^JOB.*(TITLE|PROFILE|POSITION)$` matches strings beginning with `JOB`, followed by zero or more occurrences of any character, and ending with `TITLE`, `PROFILE`, or `POSITION`.

`^[A-Z]{3}[0-9]{2}[A-Z0-9]$` matches strings beginning with three letters, followed by two digits, and ending with a letter or digit.

`BIRTH.?(COUNTRY|PLACE)|(COUNTRY|PLACE).*BIRTH` matches strings such as `BIRTH COUNTRY`, `PATIENT_BIRTH_PLACE`, `PLACE_OF_BIRTH`, and `EMPLOYEE'S COUNTRY OF BIRTH`.

Related Information

- Regular Expressions
- Boundary Matchers
- Quantifiers
- Capturing Groups

- Predefined Character Classes
- Character Classes

Introduction to Oracle Data Safe Video Transcript

This is the transcript for the Introduction to Oracle Data Safe video.

You can watch the video on Oracle Video Hub at: https://videohub.oracle.com/media/Introduction+to+Oracle+Data+Safe/1_qzygqqzb.

Introduction

Organizations rely on databases to manage their most critical asset the data. But if not well protected, this data could become their biggest liability. According to industry reports, almost one third of the attacks are performed by internal actors and over half of internal attacks are on databases. Sensitive data, such as personally identifiable information, personal financial information, and personal health care information, make databases attractive targets for hackers and even insiders who are looking to steal data for monetary, strategic or personal reasons or just to disrupt business.

By law, organizations must comply with data protection regulations, such as the European Union's General Data Protection Regulation, Payment Card Industry's Data Security Standard, Sarbanes-Oxley, and many such data protection laws across the globe. Hackers try to exploit weaknesses in user credentials, applications, and database configurations in both production and non-production databases. How do you manage against a legion of attackers who have all the infrastructure, the tools, and the time when you don't?

Oracle provides top in class security for the computing infrastructure of its databases, including encryption by default, separation of duty, and proactive security patching. But organizations need to further secure their databases by understanding their own data, their own users, and their configurations. Introducing Oracle Data Safe. A fully integrated cloud service that helps you secure your data and address compliance requirements with Data Safe.

You can assess the security of your database configurations, discover the potential risks associated with database users, find your sensitive data, mask that data in development and test environments, monitor database activity, and protect your databases against common database attacks - all from a single, easy to use database security control center.

Secure Your Databases

Poor database configurations, such as weak password policies, insufficient control of overprivileged accounts, and lack of activity monitoring, are the most common causes of database vulnerabilities. In Data Safe, Security Assessment provides you an overall picture of your database and security posture. It analyzes database configurations, users and user entitlements, and security policies to uncover security risks and improve the security posture of Oracle databases within your organization.

Security assessment provides a comprehensive assessment for your target database to help you understand potential risks. The assessment highlights remediation steps and findings related to regulations and guidelines, such as the European Union General Data Protection Regulation, Center for Internet Security and Defense Information Systems Agency Security Technical Implementation Guide, making it easier for you to identify the required security controls.

Security assessment also lets you monitor and get notified about security drift on your target databases. You get an overview of all changes of your security configurations and their corresponding risk levels.

Understand User Risks

Many questions need to be answered to understand user risks. Which database accounts have powerful roles, like database administrator, database vault administrator, or audit administrator. Who all can make changes that seriously impact the system, access sensitive data, and grant access to unauthorized users? Are some user accounts at risk of being taken over by attackers because passwords haven't been changed in a long time?

In Data Safe, User Assessment answers these questions and more to help you identify highly privileged accounts that could pose a threat if misused or compromised. Administrators can then deploy appropriate security controls and policies to ensure the ongoing security of the databases. User Assessment lets you monitor and get notified about any user or entitlement changes, and identify any weak login or password governance policies and user profiles to help strengthen your database's overall security.

Find Your Sensitive Data

Protecting sensitive data begins with knowing what sensitive data you have and where it's located in Data Safe. Data Discovery inspects the actual data in the database dictionary to find sensitive data on your target database. The search results in a sensitive data model consisting of sensitive columns estimated row counts, optional sample data for your validation and audit records. You can also view totals about your sensitive data and view the top five sensitive types.

Data Discovery includes a comprehensive and extensible library of sensitive types, which are grouped by identification, biographic, IT, financial, health care, employment, and academic information.

Mask Sensitive Data

For many applications, organizations may need to create several copies of production data to support development and test activities. If you simply copy your production data as is, your sensitive data becomes exposed to new users, increasing your attack surface. For better security, database copies should have sensitive data replaced with realistic, but fictitious, data so that even if attackers succeed in gaining access to the data, they can't benefit from the fake masked data in Data Safe.

Data Masking simplifies the job of masking data with over 80 predefined masking formats. For example, you can shuffle the data in a column, replace data with random dates, and substitute phone numbers with generic ones. You can also create your own masks.

Monitor Database Activity

You entrust your databases to your database administrators, account owners, and end users. However, it's important to monitor database activity regularly because accounts are always at risk for being hacked or misused. Activity Auditing allows you to provision and enable audit policies on your Oracle database so that you can monitor critical database changes, administrator and user activities, activities required for compliance purposes, and activities defined by your own organization.

As your audit data is generated, Activity Auditing collects your audit data and stores it in the Data Safe repository. Activity Auditing provides a wide range of interactive audit reports, each showing activities across some or all of your databases. For example, the All Activity Report is a comprehensive report that contains every audited activity and has several filter options. You can download a report as a spreadsheet or PDF file, which is useful for compliance purposes.

Generate Alerts

It's important to be alerted on certain database activities as they occur. For example, when database parameters or audit policies change; when an administrative user login fails; when users are created or deleted; when user entitlements, database schemas, or profiles change; or when SQL firewall violations occur. You can also create your own alert policies. The All Alerts report summarizes all the alerts that have been raised, including how severe is the risk? Who did what on which database? When?

You can configure OCI event notifications within Data Safe. For example, OCI sends an email when your audit trail stops. In addition, you can set up an alarm notification to let you know when an alert is triggered a specific number of times during a certain time frame.

Protect Application Data

SQL Firewall management in Data Safe helps you protect your databases against risks, such as SQL injection attacks and compromised accounts. In Data Safe, you can centrally create and manage SQL Firewall policies that restrict SQL statements and session contexts on your target databases. You can also monitor SQL being executed by users on your target databases and view SQL violations.

Conclusion

Safeguarding your data just got a whole lot easier. With Oracle Data Safe, you can secure all your Oracle databases running in Oracle Cloud, on premises, and in other cloud environments. Oracle Data Safe—ensure your critical data assets do not become a liability. To learn more, visit Data Safe's web page at `www.oracle.com/security/database-security/data-safe`.

Service Limits

Oracle Data Safe has usage and service activation limits.

Usage Limits

Usage limits are as follows:

- The combined number of security assessment, user assessment, data discovery, data masking, and audit report work requests that you can run is limited to 1000 per month per target database. If you exceed this limit, you cannot run any additional work requests for the remainder of the month. You can, however, still access Security Center and view existing reports.
- You can create up to 100 Oracle Data Safe private endpoints per tenancy and region, provided the number of unused private endpoints is below 5.*
- You can create up to five Oracle Data Safe on-premises connectors per tenancy and region.*
- Up to 1 million audit records per month per target database are included in Oracle Data Safe at no additional cost. If you exceed this limit, you may be charged for audit records over the limit. It depends on your settings in Security Center. See View and Manage Audit Profiles.
- Audit records generated by the Oracle Data Safe service user are not counted towards the monthly quota.
- Audit records are retained for up to twelve months online in Oracle Data Safe. Audit records can be archived for an additional six years (a total of seven years) in Oracle Data Safe. You can configure audit data retention periods in Oracle Data Safe.

- You can retrieve up to twelve months of audit data from the archive if archiving is configured for your target database.
- You can retrieve audit data from the archive up to six times per month per target database.

* You can create a service request to increase the limit.

Free Trial

During a free trial, the following additional limits apply:

- You can register up to one paid on-premises Oracle Database or one paid Oracle Database on a compute instance.
- You can create up to two Oracle Data Safe private endpoints.
- You can create one Oracle Data Safe on-premises connector.

For more information about using Oracle Data Safe during a free trial, see Try Oracle Data Safe for Free.