What's New for Oracle Data Safe

As soon as new and changed features become available, Oracle Data Safe is upgraded in the data centers where Oracle Cloud services are hosted. You don't need to request an upgrade to be able to use the new features—they come to you automatically. Here's an overview of new features and enhancements added recently to improve your Oracle Data Safe experience.

Date published: May 30, 2024

May 2024

Feature	Description
Pre-masking check	To prevent masking jobs from failing, you can now perform a pre-masking check to determine if your database and masking policy are ready for a data masking job. The pre-masking check performs a number of checks and provides remediation recommendations in the event a check fails. For more information, see Pre-Masking Check in the *Using Oracle Data Safe* guide.
Oracle Data Safe now supports Oracle Database@Azure	You can now register an Oracle Database@Azure as an Oracle Data Safe target database. For more information, see Register an Oracle Cloud Database in the *Administering Oracle Data Safe* guide.
On-premises connector can now be run as an OS service	You can now designate the on-premises connector as an operating system service. This designation will ensure that the on-premises connector gets automatically restarted whenever the OS of the host machine is rebooted. For more information, see Creating OS User Service for Existing On-Premises Connectors in the *Administering Oracle Data Safe* guide.
New Australian Sensitive Types and Masking Formats	New sensitive types and masking formats for Australian business, company, medicare, medicare provider, and tax file numbers have been added. For more information, see View Sensitive Types and Categories and Predefined Masking Formats in the *Using Oracle Data Safe* guide.
Additional OCI Events for Private Endpoints	Additional OCI Events for Data Safe private endpoints have been added to make it easier to know when a private endpoint is deleted. For more information, see the Data Safe Private Endpoint Event Types in the *Administering Oracle Data Safe* guide.

April 2024

Feature	Description
Additional OCI Events for Audit Trails	Additional OCI Events for audit trails have been added to make it easier to know when the status of your audit trails changes. For more information, see the Activity Auditing Event Types in the *Administering Oracle Data Safe* guide.
SQL Firewall Violation Report History	You can now view the SQL Firewall violation report history. Much like the existing Audit and Alert report history pages, the SQL Firewall violation report history page allows you to view the list of reports generated during the past three months, details about those reports, and download reports. For more information, see View and Manage Violation Report History in the *Using Oracle Data Safe* guide.
Additional filters in Report History	For easier usability, the report history pages for Audit, Alerts, and SQL Firewall Violations have been enhanced with additional filters. For more information, see View and Manage Violation Report History in the *Using Oracle Data Safe* guide.

March 2024

Feature	Description
Updated checks in Security Assessment	The Security Assessment in Oracle Data Safe was updated with additional checks from Oracle Database 19c CIS Benchmark v1.2 and STIG V2R8 for the Oracle Database as well as other updates to easier identify changes in your database's security posture. For more information, see the Security Assessment Overview in the *Using Oracle Data Safe* guide.
Create a sensitive data model manually	You can now create sensitive data models manually. This allows you to only add columns of interest to your sensitive data model instead of having to perform a discovery run and removing all unwanted columns. For more information, see Create a Sensitive Data Model Manually in the *Using Oracle Data Safe* guide.
Availability of scope information for incremental discovery	You can now view the scope details of the latest incremental discovery as well as past incremental discoveries. 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 sensitive data model. For more information, see View the History of Incremental Discovery in the *Using Oracle Data Safe* guide.

February 2024

Feature	Description
Create event notifications directly in Oracle Data Safe	You can now create event notifications and subscriptions directly in Data Safe. Instead of having to use OCI Events and Notifications to create Data Safe related Rules and Subscriptions, you can now use the **Notifications** tab available in Data Safe's features to create event notifications and subscriptions while remaining in Data Safe. For more information on creating event notifications, see, for example, Create and Modify Event Notifications in Activity Auditing in the *Using Oracle Data Safe* guide. More information about creating event notifications is available in each feature section of both the *Using Oracle Data Safe* and *Administering Oracle Data Safe* guides.

January 2024

Feature	Description
Oracle Data Safe now supports Active Data Guard associated target databases	You can now register an Active Data Guard associated database as an Oracle Data Safe target database. During target registration you can select which of the standby databases you would like to register with the primary database. In Activity Auditing you can now also collect audit records from your primary and standby databases. For more information on registering an Active Data Guard associated database, see Run the Oracle Cloud Databases Wizard in the *Administering Oracle Data Safe* guide. For more information on Activity Auditing for Active Data Guard associated databases, see View and Manage Audit Trails in the *Using Oracle Data Safe* guide. **Please note: Autonomous Database on Active Data Guard is not supported by Oracle Data Safe.**
Oracle Data Safe now supports `CDB$ROOT` target databases	You can now register a container database (CDB) as an Oracle Data Safe target database. When specifying the database service name during target registration, you can now enter the name of the CDB. For more information, see the registration workflow for your specific database in the Target Database Registration section in the *Administering Oracle Data Safe* guide.
Configure and defer risk findings	You can now manually adjust the risk level of a risk finding in a security assessment indefinitely or for a set amount of time. Additionally, a new risk level of `Deferred` allows you to indicate that you have reviewed the finding and will work on it later so that it doesn't show up again as a risk in subsequent reports. For more information, see Adjust the Risk Level of a Risk Finding in the *Using Oracle Data Safe* guide.
View user schema access details	User Assessment now 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. For more information, see View Schema Access Details for a User in the *Using Oracle Data Safe* guide.

Feature	Description
Top five security assessment findings	You can now find the top five security findings of the security assessment highlighted on top of the report and easily drill down into the details. The security assessment report shows what risk level each of these five controls was assessed at. For more information, see Structure of a Security Assessment in the *Using Oracle Data Safe* guide.

December 2023

Feature	Description
Common sensitive types	Data Discovery now makes it easy to select from the most common sensitive types instead of going through the entire list. Limiting the number of sensitive types to discover will speed up the discovery phase and also helps you to focus the scope for any subsequent data masking. For more information, see Create Sensitive Data Models in the *Using Oracle Data Safe* guide.

October 2023

Feature	Description
SQL Firewall	The SQL Firewall feature of Oracle Data Safe lets you administer and monitor SQL Firewall for your Oracle Database 23ai databases. Administrators can use Oracle 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. For more information, see SQL Firewall in the *Using Oracle Data Safe* guide.

September 2023

Feature	Description
Limited Availability of SQL Firewall	The SQL Firewall feature of Oracle Data Safe lets you administer and monitor Oracle SQL Firewall for your Oracle Database 23ai databases. Administrators can use Oracle Data Safe to collect SQL activities of database accounts, monitor the collection progress, create Oracle SQL Firewall policies with allow-list rules (allowed contexts and allowed SQL statements) from the collected SQL activities, and enable SQL Firewall policies. If you're interested in joining the limited availability program for SQLFirewall, open a service request with Oracle Data Safe with the title "Oracle SQL Firewall Limited Availability Program".

July 2023

Feature	Description
Oracle Data Safe now supports Amazon RDS for Oracle target databases	You can now register an Amazon RDS for Oracle database as an Oracle Data Safe target database. You can choose either the Oracle Data Safe on-premises connector or Oracle Data Safe private endpoint connectivity option. For more information, see Register Amazon RDS for Oracle in the *Administering Oracle Data Safe* guide.
Red Hat Enterprise Linux (RHEL) 8 support for on-premises connector installation	Installation of an on-premises connector can now be done on a host machine that runs on Red Hat Enterprise Linux (RHEL) 8. For more information, see On-Premises Connector Software Requirements in the *Administering Oracle Data Safe* guide.
Stop scheduled user and security assessments	Oracle Data Safe now provides you with the option to stop schedules for the latest user and security assessments. This can be useful if you're performing planned maintenance on a target database and don't want to receive user or security assessments for that time. Stopped schedules can easily be restarted. For more information, see Stop a User Assessment Schedule or Stop a Security Assessment Schedule in the *Using Oracle Data Safe* guide.

May 2023

Feature	Description
Oracle Data Safe guided tour	If you navigate to a region where you do not have any target databases registered a guided tour of Oracle Data Safe will automatically start. The tour provides a high-level overview of the features of Oracle Data Safe and how to start using them to improve the security of your databases. For more information, see Oracle Data Safe Guided Tour in the *Using Oracle Data Safe* guide.

April 2023

Feature	Description
User Profile insights	Oracle Data Safe now uses the user profiles that are already defined on the target database to provide you with User Profile insights. With User Profiles, you gain a comprehensive understanding of the password-related attributes associated with your Oracle Database user profiles, helping you to strengthen the system's overall security. For more information, see About User Profiles in the *Using Oracle Data Safe* guide.
Improved manageability of large sensitive data models and masking policies	New filters in sensitive data models and masking policies make it easier to explore the contents of sensitive data models and masking policies. For more information, see View Details for a Sensitive Data Model or View Details for a Masking Policy in the *Using Oracle Data Safe* guide.

Feature	Description
Compare and update a masking policy based on changes to the sensitive data model	Oracle Data Safe now allows you to compare a masking policy to the associated sensitive data model. The comparison identifies any differences between the sensitive data models and masking policy and allows you to select changes that will synchronize with the masking policy. This allows users to update an existing masking policy when new sensitive columns are discovered using incremental discovery. For more information, see Compare a Masking Policy to a Sensitive Data Model in the *Using Oracle Data Safe* guide.
Performing data masking now requires additional authorizations	Authorizations to perform data masking have been tightened to help ensure the security of your data. In order to perform data masking a user now requires `manage` permissions on the `data-safe-masking-reports` resource in the compartment of the target database. For more information, see Prerequisites for Using Data Masking in the *Using Oracle Data Safe* guide.
Option to override global paid usage and data retention settings on each target database	The ability to override global paid usage and data retention settings on each target database has been improved. For more information, see Override Global Retention Periods for a Target Database or Override Global Paid Usage for a Target Database in the *Using Oracle Data Safe* guide.
Oracle Data Safe is now automatically enabled in all regions	Oracle Data Safe is now automatically enabled in all regions when you register a target database in a region for the first time and does not require an administrator to enable on a per-region basis.
Oracle Data Safe now supports a custom listener port for Oracle Exadata Cloud@Customer target databases	When registering an Oracle Exadata Cloud@Customer target database you can now enter a custom database port number if desired. For more information, see Register an Oracle Cloud@Customer Database in the *Administering Oracle Data Safe* guide.

March 2023

Feature	Description
Advanced masking options in Oracle Data Safe	With Oracle Data Safe you can now provide the tablespace that should be used for masking, choose the level of parallel execution, if redo logs should be disabled during masking, how invalid objects will be recompiled after masking and more. These masking options can be defined when creating a masking policy or for a specific masking run. For more information on defining the masking options when creating the masking policy, see Create Masking Policies or for more information on setting and changing the masking options for a masking run, seeMask Sensitive Data on a Target Database in the *Using Oracle Data Safe* guide.

February 2023

Feature	Description
Oracle Data Safe now supports Autonomous Database on Oracle Exadata Cloud@Customer target databases	You can now register an Autonomous Database on Oracle Exadata Cloud@Customer as an Oracle Data Safe target database. You can choose either the Oracle Data Safe on-premises connector or Oracle Data Safe private endpoint connectivity option. For more information, see Register a Cloud@Customer Database in the *Administering Oracle Data Safe* guide.
Audit Insights	You can now use Audit Insights to view and analyze the audit volume of several items such as targets, schemas, and database users. 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. For more information, see Audit Insights in the *Using Oracle Data Safe* guide.
New Activity Auditing reports	Additional Activity Auditing reports have been added to Oracle Data Safe. These reports include Common User Activity, Database Error, Data Extraction Activity, and Sensitive Data Activity. For more information, see Activity Auditing Reports in the *Using Oracle Data Safe* guide.
Advanced filtering using SCIM	You can now add advanced filters to your audit or alerts reports. Advanced filters provide you with the flexibility to analyze your data using complex conditions and multiple criteria. For more information, see Advanced Filtering in an Audit Report or Advanced Filtering in Alerts Reports in the *Using Oracle Data Safe* guide.

January 2023

Feature	Description
Oracle Data Safe now supported in US Government Cloud regions	Oracle Data Safe is now supported in the US Gov West (Phoenix) and US Gov East (Ashburn) regions. For more information, see Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List in the *Administering Oracle Data Safe* guide.

December 2022

Feature	Description
History of incremental discovery	You can now view the history of incremental discoveries that were performed on your sensitive data models. This feature allows you to see when an incremental discovery was performed, what columns were added or removed, and if the changes were applied to the sensitive data model. For more information, see View the History of Incremental Discovery in the *Using Oracle Data Safe* guide.

Feature	Description
View and add previously removed columns for sensitive data models and masking policies	For both sensitive data models and masking policies, you can now view a list of columns that were previously removed. You can also add some or all of the previously removed columns back into their respective sensitive data model or masking policy. For more information, see Add Previously Removed Columns to a Sensitive Data Model and Add Previously Removed Columns to a Masking Policy in the *Using Oracle Data Safe* guide.
Bulk edit of masking formats	You can now edit the masking formats of sensitive columns in a masking policy in bulk. This feature allows you to change multiple masking formats while only having to save and update the masking policy once. For more information, see Change or Edit the Masking Format for a Sensitive Column in the *Using Oracle Data Safe* guide.
Schedule alert and Audit Activity reports	You can now create customized schedules for both alert and audit activity reports. You can specify when the report runs, how frequently the report runs, and the time span that the report covers. For more information, see Create or Change a Schedule for Alert Reports and Create or Change a Schedule for Predefined or Custom Audit Reports in the *Using Oracle Data Safe* guide.
View history of alert and Audit Activity reports	You can now view a list of the reports that were generated for both alert and audit activity reports. The history includes details about the scope of the reports, when reports were generated, and what type of reports they are. For more information, see View Alert Report History and View Audit Report History in the *Using Oracle Data Safe* guide.
Bulk alert selection	When opening or closing alerts you can now select all the filtered alerts on a page or across all pages. For more information, see Open or Close an Alert in the *Using Oracle Data Safe* guide.
Audit trail collection state filter and additional collection states	When viewing the list of audit trails, you can now filter by collection state to narrow the audit trails displayed. New collection states are also available. For more information, see Audit Trail Details in the *Using Oracle Data Safe* guide.

November 2022

Feature	Description
Custom Listener Port Number	When registering an Oracle cloud database you can now enter a custom listener port number. This includes Oracle Base Database on Virtual Machine, Oracle Base Database on Bare Metal, and Exadata on Oracle Public Cloud. For more information, see Register an Oracle Cloud Database in the *Administering Oracle Data Safe* guide
Enhancements to Incremental Discovery	When performing incremental discovery you can now alter the selected schemas and sensitive types. For more information, see Perform an Incremental Discovery of Sensitive Data on Your Target Database in the *Using Oracle Data Safe* guide.

Feature	Description
Improved adding of columns to a Sensitive Data Model or Masking Policy	When adding multiple columns to a sensitive data model or masking policy you can now specify the sensitive type of each column individually. Selecting a sensitive type for a column is now optional as well. For more information, see Add Sensitive Columns to a Sensitive Data Model and Add Columns to a Masking Policy in the *Using Oracle Data Safe* guide.
Easily remove columns from Sensitive Data Model or Masking Policy	You can now easily remove an individual column from a sensitive data model or masking policy directly from the row-specific action menu. For more information, see Remove Sensitive Columns from a Sensitive Data Model and Remove Columns from a Masking Policy in the *Using Oracle Data Safe* guide.
Update Sensitive Type of a Sensitive Column	You can now update the sensitive type of a sensitive column in a sensitive data model from the row-specific action menu. For more information, see Update Sensitive Type for a Sensitive Column in the *Using Oracle Data Safe* guide.
Change the Target Database of a Masking Policy	In the masking policy information you can now change the target database of a masking policy. For more information, see Change Target Database of a Masking Policy in the *Using Oracle Data Safe* guide.
Regulatory Filters in Security Assessment	In the Assessment Details for Security Assessments you can now filter by references including risk remediation recommendations from the Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG), Center of Internet Security (CIS) Benchmark, European Union General Data Protection Regulation (EU GDPR), and Oracle Best Practices. For more information, see Analyze Risk by using the Security Assessment Dashboard in the *Using Oracle Data Safe* guide.
Clickable User Assessment Charts	Clicking on charts in User Assessment now automatically filters the Assessment Details accordingly. For more information, see Risk Summary and Target Summary Tables in the *Using Oracle Data Safe* guide.

March 2022

Feature	Description
Oracle Data Safe now supports Exadata Cloud@Customer target databases	You can now register an Exadata Cloud@Customer database as an Oracle Data Safe target database. You can choose either the Oracle Data Safe on-premises connector or Oracle Data Safe private endpoint connectivity option.

Feb 2022

Feature	Description
The following features are now integrated with OCI: • Activity Auditing • Alerts • Data Discovery • Data Masking	All of these features have now moved to the Oracle Cloud Infrastructure Console. For more information, see the corresponding chapters in the *Using Oracle Data Safe* guide.

Nov 2021

Feature	Description
Data Safe now supported in six additional regions	Oracle Data Safe is now supported in the France 1 South (Marseille), Singapore 1, NRI Dedicated Region - Osaka, Isreal 1 (Jerusalem), Italy 1 Northwest (Milan), and UAE 2 Central (Abu Dhabi) regions. For more information, see Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List in the *Administering Oracle Data Safe* guide.

September 2021

Feature	Description
Security and User Assessment integrated with OCI	The Security Assessment and User Assessment features have moved to the Oracle Cloud Infrastructure Console. For more information, see Security Assessment and User Assessment in the *Using Oracle Data Safe* guide.
Data Safe now supported in two additional regions	Oracle Data Safe is now supported in the US DoD East (Ashburn) and US Gov East (Ashburn) regions. For more information, see Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List in the *Administering Oracle Data Safe* guide.

June 2021

Feature	Description
New Administering Oracle Data Safe guide	Oracle Data Safe security and target database registration topics have moved from the Using Oracle Data Safe guide to the new Administering Oracle Data Safe guide.
Target database registration wizards in Oracle Cloud Infrastructure	You can now perform target database registration for all supported databases via wizards in the Oracle Cloud Infrastructure Console. The Console also lets you manage and manually register target databases. The option to register an Autonomous Database from the database's detail page in Oracle Cloud Infrastructure still remains as does the ability to view registration details for target databases in the Oracle Data Safe Console. See Target Database Registration in the new Administering Oracle Data Safe guide.

April 2021

Feature	Description
Audit data lifecycle management	With audit data lifecycle management, you can now retain your audit records in Oracle Data Safe for up to seven years. See Audit Data Lifecycle Management.
Database Vault Activity report	The Database Vault Activity report shows you auditable activities of enabled Oracle Database Vault policies in target databases. See Activity Auditing Reports.

March 2021

Feature	Description
Support for Exadata Cloud@Customer databases (Limited Availability)	You can register an Exadata Cloud@Customer database by using an Oracle Data Safe on-premises connector or an Oracle Data Safe private endpoint. See Register Exadata Cloud@Customer Databases with Oracle Data Safe.

February 2021

Feature	Description
Support for Oracle databases on compute instances in non-Oracle cloud environments	With the Oracle Data Safe on-premises connector, you can now register an Oracle database on a compute instance in a non-Oracle cloud environment. See Register an Oracle Database on Compute.
Oracle Data Safe is rolled out in NRI Dedicated Region, UK Gov South (London), and UK Gov West (Newport)	Oracle Data Safe is now available in the following regions: NRI Dedicated Region, UK Gov South (London), and UK Gov West (Newport). See Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List.
New option in the Data Masking wizard: Import a file-based masking policy and use a sensitive data model from the Library	You can now import a file-based masking policy and use a sensitive data model from the Library when creating a data masking job. See Create a Data Masking Job.
Filter for compartments listed on the Authorization Policies tab	You can now filter the list of compartments on the Authorization Policies tab to show only those compartments that have grants to users in Oracle Data Safe. See Configure Authorization Policies in Oracle Data Safe.

December 2020

Feature	Description
Support for Oracle Database 11.2.0.4	Oracle Data Safe now supports Oracle Database 11.2.0.4. See **Supported Target Databases** in Target Database Registration Overview.
Support for on-premises Oracle Database via an on-premises connector	With the Oracle Data Safe on-premises connector, you can now easily register an on-premises Oracle database without needing FastConnect or VPN Connect. See Register an Oracle OnPremises Database.
Free trial support	You can now enable and try out Oracle Data Safe with a free trial in Oracle cloud. See Try Oracle Data Safe for Free.
New Data Safe Activity report	Activity Auditing has a new report called Data Safe Activity that shows you the activity generated by the Oracle Data Safe service. See Activity Auditing Reports.
Oracle Data Safe is rolled out in Chili Central (Santiago)	Oracle Data Safe is now available in the Chili Central (Santiago) region. See Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List.

November 2020

Feature	Description
Support for Oracle Autonomous JSON Database	Oracle Data Safe now supports Oracle Autonomous JSON Database. Note that the Data Discovery and Data Masking features are not supported for JSON type columns. See **Supported Target Databases** in Target Database Registration Overview.

October 2020

Feature	Description
Migration from resource groups to compartments in Oracle Cloud Infrastructure	To transition to compartments, you are prompted to perform a one-time migration when you access the Oracle Data Safe Console. During migration, you map your resource groups to compartments in your tenancy. See Migrate Resource Groups to Compartments.
Oracle Data Safe is rolled out in the UK West (Cardiff), UAE East (Dubai), and South Korea North (Chuncheon) regions.	Oracle Data Safe is now available in the UK West (Cardiff), UAE East (Dubai), and South Korea North (Chuncheon) regions. See Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List.

August 2020

Feature	Description
Support for Oracle Databases on Oracle Cloud Infrastructure Compute instances	By using an Oracle Data Safe private endpoint, you can register an Oracle database on an Oracle Cloud Infrastructure Compute instance with Oracle Data Safe. See Register an Oracle Database on Compute.
Support for on-premises Oracle Database via a private endpoint	By using an Oracle Data Safe private endpoint, you can register an on-premises Oracle database with Oracle Data Safe. See Register an Oracle OnPremises Database.
Support for Autonomous Database on Shared Exadata Infrastructure with private VCN access	By using an Oracle Data Safe private endpoint, you can register with Oracle Data Safe an Autonomous Database on Shared Exadata Infrastructure with private VCN access. See Register an Autonomous Database.
Initial audit data load	The initial audit data load feature in Activity Auditing informs you of the number of audit records that Oracle Data Safe will retreive when you start an audit trail for a target database. See Add Audit Trails and Create Activity Auditing Jobs.

July 2020

Feature	Description
Oracle Data Safe now supports Autonomous Database on Dedicated Exadata Infrastructure	Oracle Data Safe's private endpoint feature enables you to register an Autonomous Database on Dedicated Exadata Infrastructure with Oracle Data Safe. See Register an Autonomous Database.

June 2020

Feature	Description
You can schedule recurring Security Assessment jobs	You can schedule recurring security assessment jobs for one or more target databases in Oracle Data Safe. The schedule can be daily, weekly, or monthly. See Schedule Recurring Security Assessment Jobs.
Oracle Data Safe is rolled out in India Central (Hyderabad)	Oracle Data Safe is now available in the India Central (Hyderabad) region. See Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List.

April 2020

Feature	Description
Oracle Data Safe now supports Oracle Cloud databases with private IP addresses.	The new private endpoint feature in Oracle Data Safe allows you to connect your Oracle Cloud databases with private IP addresses to Oracle Data Safe. This includes ExaCS, DBCS on Virtual Machine and DBCS on Bare Metal. See Register an Oracle Cloud Database.

Feature	Description
The User Defined Functions masking format is now available with Group Masking.	Group masking enables you to mask related columns together as a group, ensuring that the masked data across the related columns retain the same relationship. In addition to the Shuffle, Deterministic Substitution, and Random Substitution masking formats, you can now also use the User Defined Function masking format for group masking. See Group Masking and Create Data Masking Jobs.
Comparison Reports are now available in Security Assessment.	Security Assessment lets you generate a Comparison Report that shows the changes on your target database between two Security Assessment reports. You can view details about database changes and risk level changes. See Comparison Reports, Baseline Reports, and Compare Comprehensive Assessment Reports.
Auto purge is no longer enabled by default.	The auto purge feature in Activity Auditing lets you purge audit records from your target databases on a regularly scheduled basis. This feature is no longer enabled by default. See Audit Data Lifecycle Management.
Additional alert policies are added to Activity Auditing.	In addition to the five predefined alert policies available in Activity Auditing, you now have two more alert policies that you can enabled: Profile Changes and Database Schema Changes. See Alerts and Alert Policies.
The Deterministic Encryption basic masking format is enhanced.	Regular expression is now an optional input for the Deterministic Encryption masking format for ASCII characters data-set. The Date data type is now supported. See Deterministic Encryption.

March 2020

Feature	Description
Service limits for Oracle Data Safe are now specified in the Using Oracle Data Safe guide.	Oracle Data Safe has usage and service activation limits. See Service Limits.

February 2020

Feature	Description
Oracle Data Safe is rolled out in Amsterdam, Jeddah, Osaka, and Melbourne.	Oracle Data Safe is now available in the Netherlands Northwest (Amsterdam), Saudi Arabia West (Jeddah), Japan Central (Osaka), and Australia Southeast (Melbourne) regions. See Add Oracle Data Safe's NAT Gateway IP Address to Your Virtual Cloud Network's Security List.
Group masking is now available in Data Masking.	Group masking enables you to mask related columns together as a group, ensuring that the masked data across the related columns retain the same relationship. See Group Masking.

January 2020

Feature	Description
Support for federated users in IAM	A federated user in Oracle Cloud Infrastructure Identity and Access Management (IAM) can now enable and use Oracle Data Safe. See Users and Groups for Oracle Data Safe.

November 2019

Feature	Description
Simplified registration for Autonomous Databases	You can now easily register an Autonomous Database from its console in Oracle Cloud Infrastructure. See Register an Autonomous Database.

September 2019

Feature	Description
Oracle Data Safe is now available in Oracle Cloud Infrastructure	Oracle Data Safe lets you assess database security configurations and database users, audit user activity, as well as discover and mask sensitive data in your Oracle Cloud databases. With Oracle Data Safe, you can protect sensitive and regulated data in those databases. For more information, see Using Oracle Data Safe.

Documentation Accessibility

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

Access to Oracle Support

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