Oracle® Session Delivery Management Cloud

Security Guide

F32607-08
February 2024

Oracle Session Delivery Management Cloud Security Guide,

F32607-08

Contents

About This Guide

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Security Guide provides information about security considerations and best practices.

The following table describes the documentation set for this release.

Document Name	Document Description
Getting Started Guide	Contains conceptual and procedural information for system provisioning and software installations.
Users Guide	Contains information about the administration and software configuration of the OSDMC.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective.
What's New	Contains a list of new features for a specific release as well as Known Issues pertaining to the release.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

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.

Revision History

This section provides a revision history for this document.

Date	Description
July 2020	• Initial release.
April 2021	• Updated for 20C April 2021 release. • Adds new chapter "Oracle SDM Cloud Cloud Security" • Adds the following sections: – "Accessing the Application" – "OCI Data Security" • Updates the following sections for accuracy: – "TLS Server Requirements" – "Secure Cloud Components with an API Key" – "Oracle SDM Cloud Data Privacy"
March 2022	• Adds the following sections: – "Traffic Flow and Firewall Port Recommendations" – "Validate Connectivity" • Moves "CCS Configuration Behind NAT or a Firewall" to "Security Overview" chapter.
August 2023	• Updated for 23C August 2023 release.
February 2024	• Updated for 24A February 2024 release.

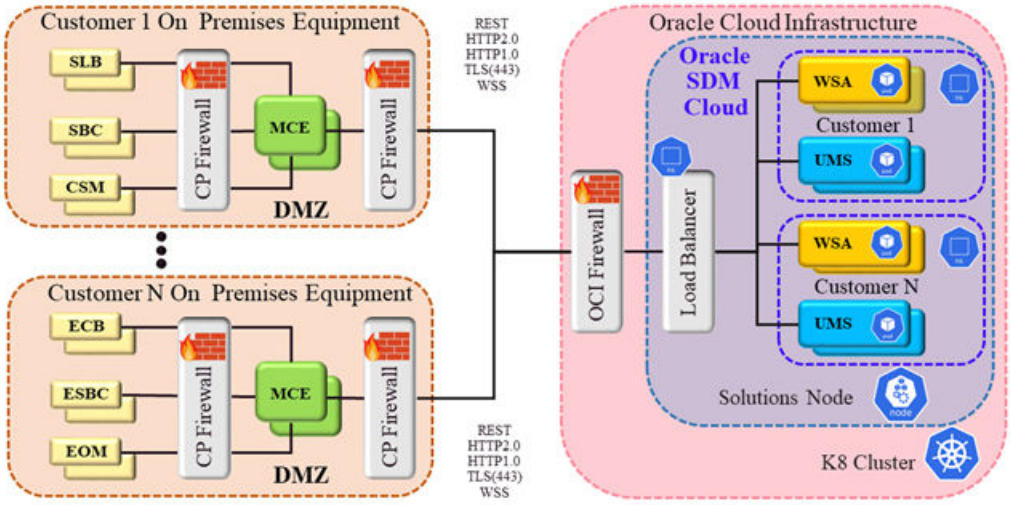
1

Oracle SDM Cloud Security Overview

Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) is a service to manage and monitor Oracle Session Delivery portfolio products residing on customer premises. The management and intelligence needed to provide this offering is maintained in the Oracle SDM Cloud micro-services hosted on the Oracle Cloud Infrastructure. For a Network Function (NF) to communicate with the Oracle SDM Cloud, the Management Cloud Engine (MCE) component must be installed on the customer premises.

The MCE component, once installed and started, registers with Oracle SDM Cloud and establishes a bi-directional web socket channel with Oracle SDM Cloud. MCE acts primarily as a protocol converter to allow REST communication to cloud to be converted to legacy protocols that the NF understand.

In the following high-level diagram of an Oracle SDM Cloud deployment integrated with the MCE, the MCE resides on premises, while the Oracle SDM Cloud micro-services reside in the Cloud.



Oracle deploys the Oracle SDM Cloud in the Oracle Cloud Native Environment, a highly secured Platform as a Service (PaaS) environment in the Oracle Cloud Infrastructure (OCI). As a result, the Oracle SDM Cloud Software as a Service (SaaS) can provide a highly secured Cloud service. The Oracle SDM Cloud solution provides high quality, highly secure Podman images for the MCE. The MCE are deployed in the customer network running on customer's platforms (Operating Systems, file systems). Such a deployment model makes security a joint effort between the customer and Oracle to ensure that the MCE runs in a secured environment. Oracle recommends that the customer ensure that their Operating System is securely hardened and that access to the customer's Operating System where the MCE runs is well managed. Unauthorized access to the MCE environments can lead to exposure of the configuration. Oracle recommends the user reserve proper resources such as memory, CPU, and network bandwidth for the MCE. For more information on these resources, see the *Oracle SDM Cloud Getting Started Guide*.

The Oracle SDM Cloud CI and CD pipeline routinely rotate client secrets for enhanced security operations. All logs, including security logs, are collected and monitored in a centralized application to detect any security violation in time.

Oracle recommends deploying the MCE in your DMZ because the MCE needs to reach out to Oracle SDM Cloud micro services (bidirectional) and IDCS for authentication. The MCE also communicates with the Session Delivery NF portfolio. It is likely that security gateways (or firewalls) are deployed before DMZs in private networks, which means that you need to configure gateways properly to allow traffic to the MCE. The MCE installation documents list the default ports, which you can modify. The port configuration is needed to configure security gateways.

For information about securing the Oracle® Session Delivery products, see the *Oracle Communications Session Border Controller Security Guide*.

Traffic Flow and Firewall Port Recommendations

The following table provides traffic flow and firewall port recommendations for all Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) components. All components use TCP and HTTPS.

Component	FQDN/IP	Port	Component Interface	Port	Notes	Communication Flow
IDCS	idcs-<Tenant Slice> .identity.oraclecloud.com	443	MCE WAN	*	MCE initiates TLS connections to IDCS	Ground-to-Cloud
Oracle SDM Cloud Load Balancer	osdmc.<region>.ocs.oraclecloud.com	443	MCE WAN	*	MCE initiates TLS connections to Oracle SDM Cloud load balancer using the OSDMC FQDN	Ground-to-Cloud

MCE Defaults

The Management Cloud Engine (MCE) server port, 7070, is hardcoded in a properties file and not configurable using the setup script. To change the value, you must manually edit the properties file.

The following are the MCE default port values:

- TRAP Receiver: 162
  The TRAP receiver port value, 162. can be changed using the setup script.

Validate Connectivity

Use the following curl commands to validate your firewall connectivity.

- From Management Cloud Engine (MCE) to IDCS

```
curl -i --noproxy "*" -X POST -u "<MCE IDCS client ID>:<MCE IDCS client
secret>" -c
"grant_type=client_credentials&scope=osdmc:premtocloud"
<IDCS_FQDN>/oauth2/v1/token
```

- From MCE to LB

```
curl -kvL4 --noproxy "*" https://osdmc.us-
ashburn-1.ocs.oraclecloud.com:443
```

Accessing the Application

Oracle's Identity Cloud Service (IDCS) supports federation/SSO external authentication, with many different Identity Providers (IDP)s. For more information, see https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/federation.htm.

2

Oracle SDM Cloud Transport Layer Security

Communications between the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) on customer premises components are protected by Transport Layer Security (TLS).

For customer tenant data, Oracle SDM Cloud uses at-rest data encryption by default, using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. For customer tenant data at rest, Oracle SDM Cloud uses the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. For customer Tenant data in-transit, Oracle SDM Cloud data encryption uses TLS 1.2+.

The Oracle SDM Cloud supports the following ciphers for on-premises TLS connections, which includes TLS connections between the MCE and Network Functions (NF)s:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

The Oracle SDM Cloud supports secure ground-to-cloud communications via TLS 1.2+. This includes the TLS connection between the on-premises Management Cloud Engine (MCE) and the Oracle SDM Cloud in the cloud.

Oracle SDM Cloud services handles the encryption keys. However, on customer premises, the customer is responsible for storing, managing, and securing the encryption keys needed for communication between MCE and NFs.

3
OCI Data Security

For information on storing cryptographic keys and general OCI data security, see https://docs.oracle.com/en/cloud/paas/database-dbaas-cloud/csdbi/data-security.html#GUID-70D37B4D-32AD-438C-8CCF-FD9F4355DA0E.

4

Secure API Key, Configuration, and Certificates Storage

The Management Cloud Engine (MCE) must be regarded as highly confidential information. Oracle recommends restricting access to admin-level users.

IDCS Authentication and Authorization

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) uses the Oracle Identification Cloud Service (IDCS) to provision your authentication and authorization credentials.

User Authentication and Authorization

During an Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) onboarding process, Oracle provisions a username and password pair for you by way of Identification Cloud Service (IDCS) . You use the username and password to access the Oracle SDM Cloud managers. Oracle recommends that you follow the IDCS guidelines for password policy and assure that only authorized personal access Oracle SDM Cloud information and manage call policies. Oracle authenticates and authorizes each request, but you must make sure that the username and password are kept safe including protection from various online security attacks

In addition, Oracle SDM Cloud provides additional authorization policies you can customize to ensure privilege access to management and monitoring capabilities that Oracle SDM Cloud offers. The following lists these features:

- Oracle SDM Cloud Security Manager is integrated with the IDCS roles and provides additional, more granular, authorization polices for you to customize what privileges your users have to monitor and manage Session Delivery Network Functions (NFs). The Security Manager also provide an Audit trail of all user initiated commands for security tracking.
- Oracle SDM Cloud Device Manager provides a centralized management of Session Delivery NF credentials, so once a NF is added, your Oracle SDM Cloud managers can have Single Sign On (SSO) access to your NF. The Session Delivery NF credentials, once entered, are encrypted in the Oracle DB and no longer accessible to the end user or to Oracle.

Ground to Oracle SDM Cloud Authentication and Authorization

During your Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) onboarding process, Oracle provisions a unique client_id and secret pair for Management Cloud Engine (MCE) per customer by way of Identification Cloud Service (IDCS). The MCE uses the client_id and secret to acquire an access token (OAuth2.0) from IDCS. The MCE uses the access token for all requests from the MCE for authentication and authorization at the Oracle SDM Cloud gate and destination micro services. The client_id and secret are very sensitive information for Oracle SDM Cloud security.

> **Note:**
>
> Ensure the client_id and secret information remains protected.
> Oracle SDM Cloud also generates a unique site identifier that the MCE uses to automatically register to Oracle SDM Cloud. Oracle SDM Cloud uses this session identifier to ensure that MCE is registering to a valid site that you have created. Oracle SDM Cloud rejects any attempt made for registration that does not match a valid site identifier. The site identifier is defined as very sensitive information for Oracle SDM Cloud security. Ensure the site indentifier information remains protected.

Oracle SDM Cloud Software Development Security

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) strictly follows Oracle Software Security Assurance (OSSA) guidelines for software development. Software security is always the top focus during software design, development, and deployment. Oracle Communications statically scans all source code and third-party software within our Continuous Integration and Continuous Delivery pipeline. Oracle Communications dynamically tests (fuzzing, penetration) all releases. All Oracle Communications Podman images pass through security and virus scans. Oracle Communications audits, fixes, or mitigates all security issues. Each Oracle SDM Cloud release is reviewed by Oracle Cloud Architecture Review (CAR), Corporate Security Solution Assurance Process (CSSAP), and verified by Security Assessment Review (SAR).

Certifications and Attestations

For information on OCI supported certificates and attestations, see https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm.

5

Oracle SDM Cloud Security Patching

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) cloud components follow the Continuous Integration-Continuous Delivery pipeline to patch any security vulnerabilities in the Oracle Cloud Infrastructure (OCI) and the Cloud Native Environment, as is Oracle's responsibility.

Security patches for the Management Cloud Engine (MCE) are a shared responsibility between Oracle and its customers. The MCE follows the Oracle Software Security Assurance requirement for handling security vulnerabilities and security fixes, which Oracle provides through the Oracle Critical Patch Update (CPU) process. Use the following link for the Oracle CPU portal: https://www.oracle.com/security-alerts/#CriticalPatchUpdates. It is the customer's responsibility to check Oracle's CPU bulletin for security patches for the MCE. If available, it is the customer's responsibility to download and apply the proper security patches.

Oracle SDM Cloud Data Privacy

Data privacy and isolation is part of the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) architecture, design, development, and operations for all customer data. When Personally Identifiable Information (PII) data is involved, Oracle SDM Cloud processes ensure that the product is compliant with the various data privacy regulations, including General Data Protection Regulation (GDPR).

In Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) components, we make sure that logging includes no PII data. Oracle either removes or anonymizes such PII data fields after a certain usage period (30 days).

The data (call records, logs, and other artifacts with PII) from Oracle SDM Cloud on-premises components (Session Delivery NF and Management Cloud Engine (MCE)) are handled according to our customer's security policies. Any data process procedures are compliant with data privacy regulations applicable to the customer's jurisdiction.

Oracle SDM Cloud supports tenant isolation. Each tenant has their own environment and instances and no compute, memory, or storage is shared for any purposes, including in testing environments.

The Oracle SDM Cloud strictly follows Oracle Software Security Assurance (OSSA) guidelines for software development. Software security is always the top focus during software design, development, and deployment. Oracle Communications statically scans all source code and third-party software within our Continuous Integration-Continuous Delivery pipeline. Oracle Communications dynamically tests (for example, fuzzing and penetration) for all releases. For more information, see https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf.

6

Oracle SDM Cloud Cloud Security

The Oracle® Session Delivery Management Cloud service (Oracle SDM Cloud) deploys in the Oracle Cloud Native Environment (CNE), which is a highly secured Platform as a Service (PaaS) environment provided by the Oracle Cloud team in the Oracle Cloud Infrastructure (OCI).

The Oracle SDM Cloud SaaS can provide a highly secured cloud service and the Oracle SDM Cloud CI/CD pipeline routinely rotates client secrets for enhanced security operations. Oracle stores all logs that the Oracle SDM Cloud collects and monitors, including security logs, in a centralized application to detect any security violation in real time.

See the Oracle Cloud Infrastructure Security Guide at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm.

On-premises Infrastructure Security

While the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) service provides high quality and secure Podman images for the Management Cloud Engine (MCE), the MCE is deployed in your network running on your platforms (for example, Operating System (OS) and file systems). It remains a joint responsibility to ensure that the MCE runs in a secured environment. Oracle recommends that you securely harden your OS, and that access to your OS, upon which MCE is running, is well managed. Inappropriate access to the MCE environments can lead to exposure of the configuration. Oracle recommends that you ensure that you reserve proper resources (memory, CPU, network bandwidth) for the MCE.

Secure MCE Deployment

The Management Cloud Engine (MCE) facilitates providing communication between Network Functions (NFs) on the customer premises (for example, SBC, ESBC, or OCSM) which are considered trusted components with the Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) services in the cloud. Because the MCE is an important component in management and monitoring of the NFs, Oracle recommends that you deploy the MCE in the DMZ and ensure that the NFs have access to it in order to ensure MCE to NF communications can be established.

Often, security gateways (or firewalls) are deployed before DMZs in private networks. In such scenarios, you must configure the gateways to properly allow traffic to the NFs and the MCE. The MCE installation documents list the default ports, which you can modify. The port configuration is needed to configure security gateways. See the *Oracle Session Delivery Management Cloud Getting Started* Guide for the default ports and installation instructions.

Oracle SDM Cloud Service Security Auditing

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) service provides user activity logging as part of the Oracle SDM Cloud Security Manager Audit logs. All user initiated activity is logged automatically in the Audit logs as part of the compliance to FCAPS, (Fault, Configuration Audit, Performance and Security). You can Audit the logs to track all

users' activities on Oracle SDM Cloud. The Audit Logs are owned by you and can only be accessed via your Oracle SDM Cloud Security Manager portal. Oracle SDM Cloud does not maintain or publish the contents of these audit logs to any internal logging system.

Oracle SDM Cloud uses a generic Identity Access Management (IAM) capability of Oracle Cloud Infrastructure (OCI) called Identity Cloud Services (IDCS). The Oracle SDM Cloud Security Manager is fully integrated with IDCS. IDCS operations can capture login, log out, and user profile changes and make them auditable.

7

Oracle SDM Cloud Data Privacy

Data privacy is on the top of Oracle's design, development, and operations whenever Personal Information data is involved to make sure our product is compliant with various data privacy regulations, including General Data Protection Regulation (GDPR). Oracle does not collect, store, or process sensitive information. In Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) Cloud components, we make sure that logging includes no PII data.

The specific data includes the Network Function (NF) (for example, SBC, SR, or OCSM), call records, and routes that Oracle SDM Cloud monitors and manages on customer premises. Any data process procedures are compliant with data privacy regulations applicable to the customer's jurisdiction. See "Appropriate Security Required by Data Privacy Regulation". For more information, see https://mosemp.us.oracle.com/epmos/main/downloadattachmentprocessor?parent=DOCUMENT&sourceId=114.2&attachid=114.1:CGBU_SESSION_DEL&clickstream=no for the *Product-Service Feature Guide* (PSFG) located in MOS under #114.2 (navigate to CGBU).

Personal Data Used by Oracle SDM Cloud

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) does not use any of this information but allows the user to retrieve it for diagnostics and specifying their routing policies for the call flows. Oracle SDM Cloud retrieves recent calls and call flow ladder diagrams, on demand, so that the user can view and diagnose call issues in their networks. The recent calls can include phone numbers, IP addresses, and device ID. In addition, the Oracle SDM Cloud route manager allows the customer to create and manage local routing tables (LRT) to control call flows in their networks. The LRT can contain phone numbers and IP addresses. LRT are stored and maintained by Oracle SDM Cloud for the user. Oracle SDM Cloud does not do any additional processing of the phone numbers or IP addresses.

Oracle SDM Cloud does not have access to store, correlate, or map restricted or sensitive personal data such as:

- End-user contact information
- Employment details HR performance details, and job qualifications
- Health and healthcare information
- Family information, lifestyle, and social circumstances
- Administrative, audit, accounting, and financial information
- Financial transaction data
- Tracking information
- Photographs and testimonials
- Call recording
- Education, qualification, curriculum vitae, resumes, and results from background checks

8
Data Encryption

Oracle encrypts data in transit and at rest and uses the Oracle Key Vault to secure keys.

Data In Transit

The Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) encrypts data in transit using TLS. See "Oracle SDM Cloud Transport Layer Security".

Data At Rest

The Oracle SDM Cloud also provides encryption of data at rest. Data at rest is stored using Oracle Data Base as a Service (DBaaS). Oracle DBaaS provides the Transparent Data Encryption (TDE) feature to address security-related regulatory compliance issues. TDE encrypts sensitive data stored in data files. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a keystore. The Oracle SDM Cloud DBaaS is configured so that the tablespaces of each PDB is encrypted. This uses a TDE master encryption key with AES-256 encryption.

Oracle Key Vault

The Oracle Key Vault stores the Oracle-held keys and distributes the keys. Key rotation is implemented automatically on a scheduled basis. (Oracle policy requires rotating keys at least annually).

Appropriate Security Required by Data Privacy Regulation

To avoid data breaches and to limit the exposure in the event of a data breach, privacy regulation requires several security measures, such as data minimization, encryption, and others.

The following table lists the security and privacy measures that Oracle® Session Delivery Management Cloud (Oracle SDM Cloud) employs to comply with data security regulations.

Security and Data Privacy Measures	**Description**
Data minimization	Oracle SDM Cloud does not manage or process the phone numbers, IP addresses, or device ID. For recent calls, this data is fetched from the user's Network Functions (NF) on customer premises for viewing and diagnostic purposes. For managing call flow routing, the user can create local route tables (LRT) and add the phone numbers to specify routing policies. Oracle SDM Cloud only provides the editor to manage the files but does not do any further processing of this data.
Deletion of Oracle SDM Cloud end-user data	Oracle SDM Cloud removes call data from the tenant when the service contract expires and you do have not or do not plan to renew the service. Oracle SDM Cloud automatically removes (destroys) personal information in the call data stored by Oracle SDM Cloud after 30 days.
Deletion of Oracle SDM Cloud customer data at contract term end or termination	Oracle SDM Cloud, along with other Oracle cloud services, utilizes Oracle Identity Cloud Service (IDCS) for subscribers to manage their user access accounts and security features. Subscribers must manage any IDCS access deletions.
End-user Data Access Request	Regarding end-users, Oracle SDM Cloud does not collect the end-users' phone numbers or IP addresses. This information is retrieved from NFs by the user when processing diagnostics. Oracle SDM Cloud does store the end-users' phone numbers and IP addresses that the customer can use in creating the LRT tables to manage call flows through their networks to provide end-users with Quality of Service (QoS). The LRTs are owned and managed by the user.
End-user request for correction and deletion for individual end-user data records	You can create, modify, and delete the phone numbers and IP addresses used to specify routing policies using the Route Manager when you have access control list privileges to do so. You can only view phone numbers and IP addresses in recent calls if you have the correct access control list privileges.

Security and Data Privacy Measures	Description
Right to be Forgotten	For Recent Call Data, neither the user nor Oracle can delete an end-user's phone number from the Oracle SDM Cloud tenant data. For LRTs, the user owns the LRT creation and can create, modify, and delete phone numbers and IP addresses for LRT. The user controls the retention policies for LRT. Oracle does not manage the LRT data.
Support multi-factor and Single Sign On authentication	Oracle Identity Cloud Service (IDCS), which is utilized by Oracle SDM Cloud, supports the ability to require Multi-FactorAuthentication as well as federated identity.
Anonymization and Pseudonymization	The personal information processed by Oracle SDM Cloud is not anonymized or pseudonymized. Oracle SDM Cloud provides the ability to view recent calls that have phone numbers and IP addresses for the purpose of diagnostics. Oracle SDM Cloud also allows you to create, modify, and delete phone numbers and IP addresses for the purpose of defining routing policies for call flows, all of which the user owns.
Masking	Oracle SDM Cloud does not add phone numbers or their associated IP addresses to Oracle SDM Cloud micro services logs.
Truncation	Oracle SDM Cloud does not process the phone numbers or IP addresses. The user owns and is responsible for truncating numbers in a managed caution list on either the NFs in their network or in routes the user creates to control call flows under Route Manager.