Oracle® Communications Security Shield Cloud Service

Security and Privacy Guide

F24353-12
August 2023

Oracle Communications Security Shield Cloud Service Security and Privacy Guide,

F24353-12

Contents

About This Guide

The Oracle Communications Security Shield Cloud Service (Security Shield) is designed to increase security when you use Oracle Cloud services with your telephony network. When properly configured, the Security Shield helps you to manage unwanted call traffic, to discover and mitigate security risks, and to monitor the system, all while providing the high service levels that your users expect from your telephony network. The Oracle Cloud Security Shield Security and Privacy Guide provides information that you need to know about installing, configuring, managing, and monitoring Security Shield operations to support security and privacy.

Documentation Set

The following table describes the documents included in the Oracle Communications Security Shield Cloud Service (Security Shield) documentation set.

Security Shield Installation and Maintenance Guide	Contains conceptual and procedural information for installing and maintaining the Security Shield.
Security Shield License Document	Contains information about the Security Shield license.
Security Shield Security and Privacy Guide	Contains conceptual and procedural information for securing the Security Shield operations.
Security Shield User's Guide	Contains the product overview along with conceptual and procedural information about using the Security Shield Dashboard.
Security Shield What's New	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.

Related Documentation

The following list describes related documentation for theOracle Communications Security Shield Cloud Service (Security Shield). You can find the listed documents on http://docs.oracle.com/en/industries/communications/.

Administrative Security Guide	Contains information about Session Border Controller support for its Administrative Security license.
SBC Family Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Session Border Controller family of products.
Oracle Cloud Infrastructure Security Guide	Contains information about maintaining your security posture in the cloud through Oracle's core pillars designed to maximize the security and compliance of the platform.

Revision History

This table provides the revision history for this document.

Date	Description
June 2020	• 20.0.0.0.0 Initial Release
July 2020	• 20.1.0.0.0
February 2021	• 20.2.0.0.0
March 2021	• Adds the "CCS Configuration Behind NAT or a Firewall" topic to the "Infrastructure Security" chapter.
June 2021	• 21.0.0.0.0
August 2021	• 21.0.0.0.0
August 2022	• 22.1.0.0.0

Documentation Accessibility

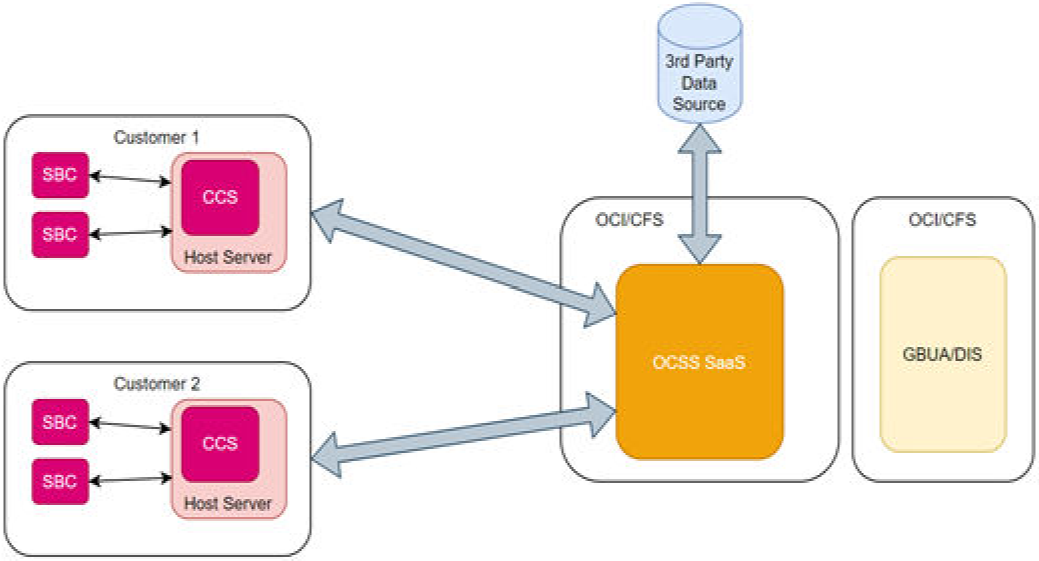
For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

1

Security Shield Security Overview

Oracle Communications Security Shield Cloud Service (Security Shield) is service that can evaluate every SIP call crossing a telephony network boundary and generate a risk assessment score for each call. The Security Shield dynamically determines the risk score for a call to provide you with an enhanced trust level for the call. The enhanced data may include a score that uses data about the caller's frequency of calls, presence on a block list or caution (suspicion) list, and reputation. To make use of the risk score, the Security Shield service contains a policy manager where you define how you want the Security Shield to respond to risky calls and sessions. The Security Shield deployment model disperses the components in a way that uses on-premises products, such as the Session Border Controller, with a cloud service overlay.

In the following high-level diagram of an Security Shield deployment, the Cloud Communication Service (CCS) and the Session Border Controller (SBC) reside on premises.



While the security for Security Shield cloud components in the Oracle Cloud is mainly Oracle's responsibility, the overall Security Shield security is a joint effort between Oracle and our customers. Especially, for the on-premises components (CCS and SBC).

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

2

Security Shield Transport Layer Security

Communications among the Session Border Controller (SBC), Cloud Communication Service (CCS), and the Oracle Communications Security Shield Cloud Service (Security Shield) cloud components, and among the Security Shield cloud components with Cloud Analytics service in the Oracle Cloud Infrastructure (OCI) and external data sources occur through the REST API and are protected by Transport Layer Security (TLS). The Security Shield service uses only TLS1.2 along with the following recommended cipher suites.

On-Premises TLS Connections

The Security Shield service supports the following ciphers for on-premises TLS connections, which includes TLS connections between the CCS and the Security Shield, and between the CCS and the SBC:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Cloud Services TLS Connections

The Security Shield service supports the following ciphers for TLS connections with Security Shield cloud services, which includes the TLS connection between CCS and OCSS cloud, and between CCS and CCS Agent:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

TLS Server Certificate Requirements

- Minimum of 2048 bits for RSA keys or 256 bits for ECDSA keys for certificates.
- Use only a strong hash algorithm for the certificate signature. (SHA256 or stronger).
- Rotate the server certificate routinely. (Yearly or less).
- Ensure that DigiCert Intermedia CA (DigiCert Global G2) with SHA256 with RSA signs the Oracle server certificates.
- Ensure that a trusted commercial CA signs the CCS server certificate facing the Security Shield cloud. Oracle ships Java SE 11 with a list of root CAs that Oracle trusts.
- Oracle recommends that either internal CA or commercial CA, per your security policy, sign the CCS server certificate facing the Security Shield and the SBC server certificate.
- Ensure that you do not use any self-signed server certificates.

Note:

Oracle ships the CCS Docker image with Oracle CA. (SHA-256 Digitizer Public ROOT and Intermediate CA certificates)

3

Secure Cloud Components with an API Key

In addition to Transport Layer Security (TLS) protection, the Oracle Communications Security Shield Cloud Service (Security Shield) authenticates the RESTful communication between the Cloud Communication Service (CCS) and the Session Border Controller (SBC) by way of a shared key called the API key. Set the API key to contain a random string of 32 to 128 printable characters long, excluding spaces and tabs. When the API key contains fewer than 32 characters, the CCS and SBC produce a warning message indicating the key is not secure. When an API key contains more than 128 characters, Security Shield generates a log message indicating that the key is too long. When the API key is too long, the OCSS uses only the first 128 characters. Oracle recommends that you rotate the API key every six months.

Oracle does not specify the tool that you use for random key generation. The following examples show how to use **openssl rand** and **uuidgen** for random byte generation.

openssl randdom -hex 16—Generates a random16 byte ID in hex (32 characters). For example:

```
$ openssl rand 16 -hex16
cdb18eae600b3d4d837fb6f23b8bf90e
```

uuidgen -r—Generates a random 16 byte ID that you can use for the API key. Remove "-s" before using it for the API key. For example:

```
#create random uuid
$ uuidgen -r
a68eddcd-6eec-4b5e-846d-97b1161248e2 (Remove the hyphens "-" to result in
the following key: a68eddcd6eec4b5e846d97b1161248e2)
```

Secure API key, Configuration, and Certificate Storage

Oracle recommends that you regard the API-Key, the Cloud Communications Service (CCS) configuration, the CCS certificate and its associated private key as highly confidential information. Oracle recommends that you restrict access to admin-level users.

4 Security Shield Authentication and Authorization by IDCS

The Oracle Communications Security Shield Cloud Service (Security Shield) uses the Identification Cloud Service (IDCS) to provision your authentication and authorization credentials.

User Authentication and Authorization

During a your Security Shield on-boarding process, Oracle provisions a user name and password pair for you by way of IDCS. You use the user name and password to access the Security Shield Dashboard. On the Dashboard you can administer and manage call policies and view various call statistics through web browsers. IDCS(Oauth2.0) manages and verifies the user name and password. Oracle recommends that you follow the IDCS guidelines for password policy and assure that only authorized personal access Dashboard information and manage call policies. Oracle authenticates and authorizes each request, but you must make sure that the user name and password are kept safe including protection from various online security attacks.

Ground to Security Shield Authentication and Authorization

During your Security Shield on-boarding process, Oracle provisions a unique client_id and secret pair per Cloud Communication Service (CCS) per customer by way of IDCS. The CCS uses the client_id and secret to acquire an access token (OAuth2.0) from IDCS. The CCS uses the access token for all requests from the Session Border Controller through the CCS for authentication and authorization at the Security Shield gate and destination micro services. The client_id and secret are very sensitive information for Security Shield security. Protect this information.

Security Shield Cloud to Ground Authentication and Authorization

The Security Shield communicates with the CCS deployed in your network for call policy and mid-call updates. The requests from Security Shield include an access token from IDCS. The CCS authenticates and authorizes the requests by way of the access token. In this scenario, the CCS uses its client_id and secret to acquire the IDCS server certificate to verify the signature of the access token.

You must manage user access and account deletions. IDCS does not.

For more information about IDCS and IDCS configuration, see: https://docs.oracle.com/en/cloud/paas/identity-cloud/index.html

5

Security Shield Software Development Security

The Oracle Communications Security Shield Cloud Service (Security Shield) 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 (fuzzing, penetration) all releases. All Oracle Communications Docker images pass through security and virus scans. Oracle Communications audits, fixes, or mitigates all security issues. Each Security Shield release is reviewed by Oracle Cloud Architecture Review (CAR), Corporate Security Solution Assurance Process (CSSAP), and verified by Security Assessment Review (SAR).

Security Shield Security Patching

The Oracle Communications Security Shield Cloud Service (Security Shield) cloud components follow the Continuous Integration-Continuous Delivery pipeline to patch any security vulnerabilities in the Oracle Cloud Infrastructure and the Cloud Native Environment, as is Oracle's responsibility. Security patches for the Cloud Communication Service (CCS) are a shared responsibility between Oracle and its customers. The CCS 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 your responsibility to check Oracle's CPU bulletin for security patches for the CCS and download and apply the proper security patches.

6
Security Shield Cloud Security

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

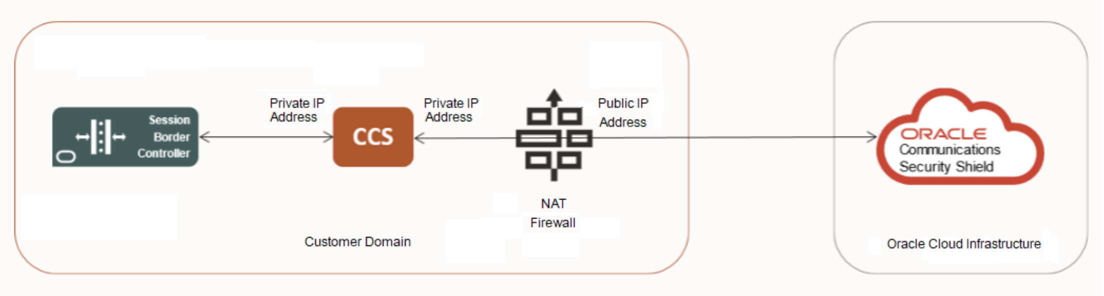
See the *Oracle Cloud Infrastructure Security Guide* at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm.

On-premises Infrastructure Security

While the Oracle Communications Security Shield Cloud Service (Security Shield) provides a high quality and secure docker image for the Cloud Communication Service (CCS) deployed in your network and running on your platforms (for example, Operating System (OS) and file systems). It remains a joint responsibility to ensure that the CCS runs in a secured environment. Oracle recommends that you securely harden your OS and that access to your OS, upon which CCS is running, is well managed. Inappropriate access to the CCS environment can lead to exposure of the configuration, private keys, and PI-keys. Oracle recommends that you ensure that you reserve proper resources (memory, CPU, network bandwidth) for the CCS.

CCS Configuration Behind NAT or a Firewall

Oracle recommends that you configure the Cloud Communication Service (CCS) to operate behind Network Address Translation (NAT) or a firewall.


Session Border Controller
Private IP Address
CCS
Private IP Address
Public IP Address
NAT Firewall
Customer Domain
ORACLE Communications Security Shield
Oracle Cloud Infrastructure

Oracle designed the Oracle Communications Security Shield Cloud Service (Security Shield) to contact the CCS using the value for the **"Server-FQDN"** configuration field in the CCS. The CCS supplies the **"Server-FQDN"** value when it registers with Security Shield. For example:

```
“Server-FQDN” : “ccs.useast.example.com”
```

You can set the **"Server-FQDN"** value as an FQDN or a static IP address that maps to the public interface of the NAT or firewall. Security Shield always uses port 443 for these connections, which requires any device placed between the CCS and Security Shield to dedicate port 443 to the CCS for all possible IP addresses resolved for the FQDN.

Security Shield Service Security Auditing and Detective Control

The Oracle Communications Security Shield Cloud Service (Security Shield) provides user activity logging. Activity logging records admin activities and settings changes, such as configuration modification, adding devices, and creating, deleting, and modifying Access Control Lists. You can use the activity log for audits.

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

7 Security Shield 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 Communications Security Shield Cloud Service (Security Shield) Cloud components, we make sure that logging includes no PII data. For the data sent to external partners for verification, we make sure that all Security Shield partners comply with data privacy regulations. For the data sent to Oracle data analytics service, all data fields identified as PII are marked properly. Oracle either removes or anonymizes such personal information data fields after a certain usage period (30 days).

The specific data includes phone number, IP address, and device type identifier that may appear in call records, logs, and other artifacts from Security Shield on-premises components (Session Border Controller and Cloud Communication Service) 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. See Appropriate Security Required by Data Privacy Regulation.
For more information, customers with a My Oracle Support (MOS) contract or who are under a Non-disclosure Agreement can refer to the *Product-Service Feature Guide* (PSFG) located in MOS under #114.2 (navigate to CGBU).

Personal Data Used by Security Shield

The Oracle Communications Security Shield Cloud Service (Security Shield) uses only the metadata from call signaling, such as the phone numbers. Security Shield uses both the calling number and the called number to assess the risk of a phone call and the phone number. The call signaling may include device identifiers, for example, IP addresses, device ID, and device fingerprints. When these identifies are available, Security Shield stores them as part of the call data for a call. Security Shield does not record calls.

Security Shield 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 Communications Security Shield Cloud Service (Security Shield) encrypts data in transit using TLS. See Security Shield Transport Layer Security.

Data At Rest

The Security Shield 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 Security Shield 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).

A

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. Oracle Communications Security Shield Cloud Service(Security Shield)

Table A-1

Security and Data Privacy Measures	Description
Data minimization	Security Shield processes only header information from SIP INVITE and BYTE messages and considers only information in the call signaling, such as phone numbers and IP addresses.
Deletion of Security Shield end-user data	Security Shield removes call data from the tenant when the service contract expires and you do have not or do not plan to renew the service. Security Shield automatically removes (destroys) personal information in the call data stored by Security Shield after 30 days.
Deletion of Security Shield customer data at contract term end or termination	Security Shield, 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, Security Shield collects only the end-user's phone number, name, and IP addresses. Each entry is stored for a period of 30 days. Using the Analysts reports the you can find all records for a given phone number, noted in the third URL.
End-user request for correction and deletion for individual end-user data records	You can modify the related configuration through the Security Shield Dashboard and you can put an end-user's phone number on an allow-list using the Access Control list capability as noted in the second URL. You cannot delete individual entries, as noted in the first URL.
Right to be Forgotten	Neither you nor Oracle can delete an end-user's phone number from the Security Shield tenant data. When the Security Shield tenant does not see a phone number for 30 days, it automatically removes the tenant data.
Support multi-factor and Single Sign On authentication	Oracle Identity Cloud Service (IDCS), which is utilized by Security Shield, supports the ability to require Multi-FactorAuthentication as well as federated identity.

Table A-1 (Cont.)

Security and Data Privacy Measures	Description
Anonymization and Pseudonymization	The personal information processed by Security Shield is not anonymized or pseudonymized. Security Shield requires the phone numbers to be available in call signaling. Device identifier and IP address may be used as well. No other personal information is collected or stored.
Masking	Security Shield masks phone numbers when added to Security Shield microservices logs. You cannot access these logs.
Truncation	Security Shield truncates the numbers on an Oracle managed caution list. These numbers typically reflect high cost destination or high risk destinations such as so-called Premium Rate Service Numbers, for example, 900 numbers in the U.S.

B

Security Shield Security Frequently Asked Questions

The following table lists some frequently asked questions about the Oracle Communications Security Shield Cloud Service (Security Shield) and security.

Table B-1

Question	Answer
What are the encryption algorithm, key length, and rotation frequency for Security Shield data at rest in the Oracle Cloud Infrastructure?	The Oracle Database feature Transparent Data Encryption (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 Security Shield Data Base as a Service (DBaaS) is configured so that the tablespaces of each PDB are encrypted. Each PDB uses a TDE master encryption key with AES-256 encryption. Security Shield uses the Oracle Key Vault to store the Oracle held keys and to distribute the keys. Oracle rotates the keys automatically on a scheduled basis for all CDBs and PDBs. Oracle policy requires rotating keys at least annually.
Are Security events recorded and auditable, especially the events in the list show here?	• Log in and Log out • Access to restricted data • Profile changes • Admin activities • Settings changes • Logging changes • Access to protected data Security Shield uses a generic Identity and Access Management capability of the Oracle Cloud Infrastructure called Identity Cloud Service (IDCS). IDCS provides operations that capture log in, log out, and user profile changes and makes them auditable. The Security Shield provides user activity logging, which records admin activities and settings changes, such as configuration modification, adding, deleting, and modifying devices, and creating, deleting, and modifying Access Control Lists. You can use the activity log for audits. Security Shield users do not have access to restricted or protected data other than phone numbers. Phone numbers are used to identify the target or source of a fraud attempt, nuisance incident, or a potential security incident.

Table B-1 (Cont.)

Question	Answer
How does Security Shield protect user Privacy information?	Security Shield processes only header information from SIP INVITE and BYTE messages. Any data fields classified as PII Personal Identifiable Information (PII), such as phone numbers and IP addresses, are removed in 30 days after which the data then will no longer retrievable.
Does Security Shield access end user's critical, sensitive information like credit card numbers, account numbers, PINs, and health information?	Security Shield processes only SIP signaling messages. It does not have access to media streams, including DMTF. Security Shield does not have access to restricted and protected information such as credit card numbers, account numbers, PIN, health information.
Can access to the Security Shield management portal be restricted to specific IPs?	Security Shield Identity Access Management is supported by Oracle Identity Cloud Service (IDCS). IDCS supports Assertion Grant Type (OAUTH2). But further work is needed for federation integration for Security Shield.
Can we federate authentication into the OCSS management portal? PingFederate, SAML?	No.
Does the OCSS management portal support multi-factor authentication?	Multi-factor authentication is supported by IDCS and can be integrated with Security Shield.
Does Oracle maintain "Break Channel" accounts that allow them to manage the service without seeing our data?	General service management is done without access to the customer data. The only way Oracle could have access is viatenant provided credentials to the customer's PDB which would only be used for very specific actions.
Can we bring our own encryption keys? If yes, how to rotate these keys?	No, Security Shield does not use static encryption keys with hard-coded algorithms.
Can we bring our own certificates?	Yes. TLS certificates must be supplied and configured by the customer for on-premises SW (SBC and CCS). The Cloud Communications Service (CCS) server certificate for TLS-interface facing Oracle Cloud (between CCS and OCSS cloud) should be signed by a trusted CA. Oracle manages the TLS certificates for Security Shield TLS interfaces, which are signed by the Oracle CA (a digicert CA).
Can we rotate the certificates?	Yes. Oracle recommends to rotate your certificates every 6 months, at minimum, or every 12 months. Security Shield cloud certificates are required to be rotated annually.
Does the management portal support...	• Role Based Access (RBAC): Not supported at this time. • Users and groups: Partially supported st time. • Entitlement reviews: Currently user have all entitlements. • Setting password policies (length, content, expiration) Yes; supported through Oracle IDCS (OCI IAM).
Is data stored in the cloud encrypted at rest?	Yes. TDE (Oracle Transparent Data Encryption) is used with strong ciphers like AES-256.

Table B-1 (Cont.)

Question	Answer
Can subscribers back up and restore configurations made in the cloud?	No. Security Shield internally backs up configurations and restores them when needed.