Oracle® Communications Session Border Controller and Session Router

Release Guide

Release 7.4.1M1

December 2018

ORACLE

Oracle Communications Session Border Controller and Session Router Release Guide, Release 7.4.1M1

Copyright © 2014, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

About this Guide

1 S-Cz7.4.1M1

Platform Support for S-Cz7.4.1M1 1-1
Upgrade Information 1-1
Supported SPL Engines 1-2
Neighbor Release Patch Equivalency 1-3
New in this Release 1-3
- Lawful Intercept Configuration Encryption 1-3
- SHA-2 Authentication-Password Hashing 1-6
- Bootparam Security 1-6
- SFTP Access Restrictions 1-6
- Import Private SSH Key to Derive New SSH Host Keys 1-7
- Import a Private SSH Key for the OCSBC as an SFTP Client 1-7
- Delete an SSH Key 1-9
- Securing Communications Between the OCSBC and SDM with TLS 1-9
- AAA Authentication For ACP 1-10
- SIPREC Removed 1-10
- Deprecated Ciphers 1-10
- Known Issues in S-Cz7.4.1M1 1-10

About this Guide

Overview

This Release Guide document provides an introduction to the release and an overview of the new features provided with this release.

The S-CZ7.4.1M1 release runs as either the Oracle Communications Session Router and Oracle Communications Session Border Controller. The user can setup the software as either product.

Refer to the S-CZ7.4.0 Release Notes for a summary of applicable known issues, caveats, behavioral changes, and feature deprecation.

> **Important:**
>
> This software supports LI functionality. When implementing this product, France-based users must consider the regulations, especially the R266 regulations, in the Code pénal.

Related Documentation

The following table lists the members of the Session Router S-CZ7.4.0 documentation set (http://docs.oracle.com/cd/E81292_01/index.htm) that apply to this release:

Document Name	Document Description
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500.
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3820.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Service Provider Oracle Communications Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.

Document Name	Document Description
Maintenance and Troubleshooting Guide	Contains information about Oracle Communications Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Communications Session Border Controller's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the Oracle Communications Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Communications Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Border Controller family of products.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.

Revision History

This section contains a revision history for this document.

Date	Description
January 2018	• Initial Release
March 2018	• Adds issue wherein an OCSBC downgrade allows for SIPREC operation on an inappropriate version
September 2018	• Adds "Known Issues in S-Cz7.4.1M1".
December 2018	• Adds "Deprecated Ciphers".

1

S-Cz7.4.1M1

This section acts as Release Notes for S-Cz7.4.1M1. Maintenance Release content supercedes that distributed with the point release. This release is specific for customers in France. This release is compliant with the R226 law.

Platform Support for S-Cz7.4.1M1

The following platforms support the S-Cz7.4.1M1 version of the OCSBC:

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300

The following platforms support the S-Cz7.4.1M1 version of the OCSR:

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300

The S-Cz7.4.1M1 version of the OCSR has restricted support for the following platforms:

- HP DL360 G8
- HP DL360 G9

Upgrade Information

This section provides key information about upgrading to this software version.

Supported Upgrade Paths

The following upgrade paths are supported:

- S-CZ7.3.0 -> S-CZ7.4.1M1
- S-CZ7.4.0 -> S-CZ7.4.1M1

When upgrading to this release from a release older than the previous release, read all intermediate Release Notes documents for notification of incremental changes.

Upgrading Systems that have SIPREC Enabled

This software version does not support SIPREC. If upgrading to this version of software from a system that has the SIPREC feature enabled, perform the following steps prior to upgrading:

1. Execute the **setup entitlements** command to disable the **SIPREC Session Recording** feature. For HA deployments, disable this entitlement on both the active and backup OCSBCs.
2. Execute the **show entitlements** command to ensure **SIPREC Session Recording** is disabled.
3. Execute the **Save** and **Activate** commands. For HA deployments, execute these commands on the active OCSBC.
4. For HA deployments, wait for the configuration to be synchronized to the backup. You can use the **show health** command to verify synchronization.
5. Perform the software upgrade.

Supported SPL Engines

The following SPL engine versions are supported by this S-Cz7.4.1M1 software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C2.3.2
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.0.7
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6
- C3.1.7
- C3.1.8

Neighbor Release Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This assures you that in upgrading, defect fixes in neighbor stream releases are included in this release.

Neighbor Release Patch Equivalency for S-Cz7.4.1m1:

- S-Cz7.4.0m1p1
- S-Cz7.4.0m1p2

The patch baseline, the most recent patch build from which the GA build was created, is SCZ741 GA.

New in this Release

This section presents new features included in the S-Cz7.4.1M1 release. This release is for Oracle Communications Session Router (OCSR) and the Oracle Communications Session Border Controller (OCSBC).

- LI Configuration and Backup Encryption
- SHA-2 Account-Password Hashing
- Boot Flag Security
- SFTP Access Restrictions
- SFTP Key Import
- SDM Communications Link over TLS
- SIPREC Removed - This software version does not support SIPREC.

Release Specifications

See the S-Cz7.4.0 Release Notes for release specifications.

> **WARNING:**
>
> Exceptions to the S-Cz7.4.0 specifications include, if the user chooses to change passwords, this version (S-Cz7.4.1M1) is only compatible with Oracle Communications Session Delivery Manager (OCSDM) version 8.1 and later for OCSBC and OCSR products.

-

Lawful Intercept Configuration Encryption

The li-admin user can encrypt the lawful intercept configuration with a password. The configuration elements not related to lawful intercept remain unencrypted.

Oracle recommends using this feature for increased security. After enabling this feature, the li-admin user should make a backup of the configuration file.

> **WARNING:**
>
> Once this feature is enabled, the Oracle Communications Session Border Controller can not use lawful intercept configurations that are unencrypted or encrypted with a different passphrase. If users attempt to load a configuration file that is unencrypted or encrypted with a different password, the OCSBC will ignore the LI configuration when loading the file.

This feature is not backwards compatible. Lawful intercept configurations encrypted by the OCSBC cannot be loaded on to systems running a previous software version that does not support this feature. However, lawful intercept configurations may always be recreated from the ACLI, and configuration files that do not contain lawful intercept parameters can still be loaded across multiple OCSBCs running this version.

Enable this feature by setting the passphrase with the **secret li-config** command. The passphrase must be between 8 and 64 characters and contain 3 of the 4 character classes:

- lower case letters
- upper case letters
- numerals
- punctuation

The screen does not display the passphrase.

```
ORACLE(li-admin)# secret li-config

-----------------------------------------------
WARNING:
Proceed with caution!
Changing the LI configuration encryption password will make any
previous backup/archive configuration file unusable.
The proper procedure is :
  1. Change the password in standby SBC
  2. Change the password in active SBC
  3. Do Save and activate in active SBC
  4. Take the backup of the configuration

-----------------------------------------------

Are you sure [y/n]?: y
Enter New Password:
Confirm New Password:

Password is acceptable.

-------------------------------------------
WARNING:
Li-configuration password has been updated,
run 'save-config' and 'activate-config' commands to
commit the changes now.
Take the backup of the configuration.

-------------------------------------------
%% Success
ORACLE(li-admin)#
```

The passphrase can also be reset with the same command.

HA Mode

To enable this feature in a high availability environment:

1. Set the passphrase on the standby node.
2. Set the passphrase identically on the active node.

> **WARNING:**
>
> If the passphrase of the active and standby nodes do not match, a failover will disrupt lawful intercept.

3. Save and activate the configuration in the active node.
4. Create a backup of the configuration.

Upgrades

When upgrading to a software version that supports lawful interface configuration encryption, the OCSBC loads the unencrypted backup configuration during start-up. If no passphrase is set, the lawful intercept configuration remains unencrypted and the OCSBC writes a warning in the audit log.

If downgrading to a previous version that does not support this feature, the OCSBC will only load an unencrypted lawful intercept configuration.

Alarms and Logging

If the li-admin user enabled this feature by setting the passphrase and the admin user loads a backup configuration file with an unencrypted lawful intercept configuration, all of the configuration elements will load except the lawful intercept configuration elements. If this happens, the OCSBC writes a warning to the audit log.

If the li-admin user has not enabled this feature, an unencrypted backup configuration can be loaded but a warning message will be written to acme.log.

Alarms are generated in the following situations:

- If the li-admin user has set the passphrase and a user attempts to load an unencrypted backup configuration, the OCSBC rejects the configuration and generates a 'Failed to decrypt' alarm only visible to the li-admin user.
- If the li-admin user has set the passphrase and a user attempts to load a configuration encrypted with a different passphrase, the OCSBC rejects the configuration and generates a 'Failed to decrypt' alarm only visible to the li-admin user.

Session Delivery Manager

Versions of the Session Delivery Manager that support this release can send and receive the encrypted lawful intercept configurations and backup configurations using the ACP protocol.

SHA-2 Authentication-Password Hashing

The Oracle Communications Session Border Controller supports SHA-2 hashing of user login passwords. The OCSBC hashes passwords using a randomly generated salt with 65532 iterations of the SHA-512 algorithm.

Enabling SHA-2 Password Hashing

Passwords are changed with the **secret login** command. All newly set passwords are hashed with SHA-2, the SHA-1 hash is removed, and thereafter the OCSBC uses SHA-2 to validate the password for that user. Oracle recommends that all users change their passwords after upgrading the system.

> **WARNING:**
>
> Regarding upgrades to this software, versions of Session Deliver Manager prior to SDM 8.1 do not support managing SHA-2 enabled OCSBCs. To manage an OCSBC, you must use SDM 8.1 with basic authentication.

> **WARNING:**
>
> If you downgrade to a release that only supports SHA-1 hashing after a user login password has been SHA-2 hashed, users will be locked out until all passwords are cleared. To clear passwords, contact Oracle Support.

Bootparam Security

An Oracle Communications Session Border Controller ignores attempts to modify security related boot flags from the ACLI. The OCSBC still supports changing security related boot flags through the bootloader.

Table 1-1 Security Related Boot flags

Boot flag	Description
0x00000001	Disable all security filtering on all network interfaces
0x00000010	Enable direct Linux login on port 2200 via SSH for debugging
0x00000020	Enable the debug console
0x01000000	Enable SFTP access to protected files and directories
0x20000000	Enter failsafe mode
0x40000000	Boot directly to the Linux shell

SFTP Access Restrictions

In the default restricted mode, the normal user and admin user are restricted from adding, deleting, renaming, or modifying sensitive system files when accessing the file system with SFTP. Although setting the boot flag to `0x01000000` allows access to sensitive files, if the

ANSSI R226 Compliance entitlement is enabled, all boot flags are reset to zero during a reboot and can only be set through the bootloader.

Import Private SSH Key to Derive New SSH Host Keys

The Oracle Communications Session Border Controller supports importing externally generated SSH keys to replace the internally generated SSH host keys. Because the OCSBC derives the public key from the private key, only the externally generated private key needs to be imported. The OCSBC uses these keys when it functions as an SSH server. The OCSBC supports RSA or DSA key lengths of 1024, 2048, 3072, or 4096 bits.

1. Connect to the OCSBC as the admin user.

   ```
   ssh admin@10.0.0.1
   ```

2. Run the **ssh-priv-key import host-key** command.
3. Paste the private key into the console in RFC 4716 format, followed immediately with a semicolon.

   ```
   ORACLE# ssh-priv-key import host-key
   Import externally generated SSH host key pair

   IMPORTANT:
           Please paste SSH private key in the format defined in RFC 4716.
           Terminate the key with ";" to exit.
   -----BEGIN RSA PRIVATE KEY-----
   MIIEpAIBAAKCAQEAxd3bGH0tlLlaLmA35uveUhgRuoxgt1KSSn4ZrBXKuRam4ILO
   ++16Qn0kYVmCfxKpYhaQ3LcTOeR+/WRV4uVp5RNPw4QRTSUdMjhODt8yxy22rHrW
   .
   .
   .
   tbNEZ7oOKBhLmdO9WvU1OqBumZmV+TtI8jdEzn1T0ZJZ45mTEtJjMwv00VHh94t4
   Lye/a8t/dV4+HvBMfCY2SKnDivLJAWWFlPz6NhSk6qUaNwReytL9CQ==
   -----END RSA PRIVATE KEY-----;

   SSH host key imported successfully.
   ORACLE#
   ```

   > **Note:**
   >
   > Do not insert a new line character before the terminating semicolon.

   The OCSBC only supports one set of SSH host keys. Importing a second host key overwrites the previous pair. Use the **ssh-priv-key delete host-key <key-type>** command to overwrite the current host-key with an internally generated host-key.

Import a Private SSH Key for the OCSBC as an SFTP Client

As an alternative to relying on the SSH keys generated by the Oracle Communications Session Border Controller, customers may import externally generated SSH keys for any configured **public-key** element. Because the OCSBC derives the public key from the private key, only the private key needs to be imported, and any previously generated keys for this **public-key** element will be overwritten. The OCSBC uses these keys when it functions as an SFTP client.

1. Access the **public-key** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# public-key
ORACLE(public-key)#
```

2. Set the parameters for this configuration element.

   - **name**—A record name for this public key.
   - **type**—The key type. Supported values are `rsa` and `dsa`.
   - **size**—The size of the public key in number of bits. Supported values are 512, 1024, 2048 and 3072.

```
ORACLE(public-key)# name acme
ORACLE(public-key)# type rsa
ORACLE(public-key)# size 1024
```

3. Type **done** when finished and return to the top-level element.

```
ORACLE(public-key)# done
public-key
        name                                    acme
        type                                    rsa
        size                                    1024
        last-modified-by                        admin@10.0.0.1
        last-modified-date                      2017-11-07 14:04:49

ORACLE(public-key)# exit
ORACLE(security)# exit
ORACLE(configure)# exit
ORACLE#
```

4. Save and activate your configuration

> **Note:**
>
> The **verify-config** command reports an error about a missing public key. You may ignore this error.

5. Run **ssh-priv-key import <record-name>** and paste the private key into the console in RFC 4716 format, followed immediately with a semicolon.

   Use the value of the **name** parameter for the value of **<record-name>**.

```
ORACLE# ssh-priv-key import acme

IMPORTANT:
        Please paste SSH private key in the format defined in RFC 4716.
        Terminate the key with ";" to exit.

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAx7DC2/A8zrhhHxcLw6CBLGKaVSWc2jJBnBZNayCd+L5gvJl/
eAYXqMwwByoL1CxIcNIYvRd76DNtnpvaGjcHoXjT0OJD12ps6yZz02NJz2IznQtP
.
.
.
m8D2P8lc22Tw2GBfmRsJdktvA2GM4e4RhWQcyOtcee4Sw2E8HzxCvSM0hv4SArEo
jWzbxmOdHaGIs22F25kp/0N2D12rg1DZn5QaMoNPY+A0nODw0+I+
-----END RSA PRIVATE KEY-----;
```

```
SSH private key imported successfully....
WARNING: Configuration changed, run "save-config" command to save it
and run "activate-config" to activate the changes
ORACLE#
```

> **Note:**
>
> Do not insert a new line character before the terminating semicolon.

6. Save and activate the configuration.

Delete an SSH Key

You can delete private keys from the system individually.

1. Use the **ssh-priv-key delete <record-name>** command to delete a previously created or imported SSH key pair. In the example below, the key's record name is 'acme'.

   ```
   ORACLE# ssh-priv-key delete acme
   SSH public key deleted successfully....
   WARNING: Configuration changed, run "save-config" command to save it
   and run "activate-config" to activate the changes
   ORACLE#
   ```

2. Save and activate your configuration.

> **Note:**
>
> If you delete this imported key, the OCSBC will generate its own.

Securing Communications Between the OCSBC and SDM with TLS

You can use the Transport Layer Security (TLS) protocol to secure the communications link between the Oracle Communications Session Border Controller (OCSBC) and the Oracle Communications Session Delivery Manager (SDM). Note that the systems use Acme Control Protocol (ACP) for this messaging.

To configure the OCSBC to use TLS for this ACP messaging:

1. Configure a TLS profile. The tls-profile object is located under security, where you add certificates, select cipher lists, and specify the TLS version for each profile.
2. Configure system-config element's `acp-tls-profile` parameter to specify this TLS profile.

The `acp-tls-profile` parameter is empty by default, which means that ACP over TLS is disabled. When ACP over TLS is disabled, the SDM establishes a TCP connection with the OCSBC. When the `acp-tls-profile` parameter specifies a valid TLS profile, the OCSBC negotiates a TLS connection with SDM.

> **Note:**
>
> This feature requires SDM version 8.1 and above.

AAA Authentication For ACP

To authenticate SDM by way of an external AAA server connected to the OCSBC, the OCSBC supports ACP authentication using the HTTP Basic Authentication Scheme. By using ACP over TLS, the OCSBC exchanges RADIUS or TACACS+ encrypted passwords and shared keys securely.

This functionality requires a TLS profile and the assignment of that profile under the **system-config** using the **acp-tls-profile** parameter.

> **Note:**
>
> This feature requires SDM version 8.1 and above.

SIPREC Removed

This software version does not support SIPREC. Do not enable the **SIPREC Session Recording** entitlement on this software version. Refer to the Upgrade section in this document for information on Upgrading Systems that have SIPREC Enabled.

Deprecated Ciphers

The OCSBC deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers:

- All DES-CBC ciphers, including:
  - TLS_DHE_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA

The user should remove any prior Oracle Communications Session Border Controller version configuration that used these ciphers, and not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the **ALL** (default) value to the **cipher-list** parameter no longer use these ciphers.

> **Note:**
>
> Your version of the ACLI may still print these ciphers when you run **cipher-list ?**. Despite printing them in ACLI output, the system does not support them within service operations.

Known Issues in S-Cz7.4.1M1

The following table lists S-Cz7.4.1M1 Known Issues.

ID	Description	Found In	Fixed In
28650852	The SBC changes the value of the P-Early-Media header in a 183 message to the sip-interface's **p-early-media-direction** parameter setting.	SCZ741m1	

Note:

For a complete list of Known Issues related to this release, see the *S-Cz7.4.0 Release Notes*.