## Contents

### About this Guide

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

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acme Packet 4500 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 4500.</td>
</tr>
<tr>
<td>Acme Packet 3820 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 3820.</td>
</tr>
<tr>
<td>Acme Packet 4600 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 4600.</td>
</tr>
<tr>
<td>Acme Packet 6100 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 6100.</td>
</tr>
<tr>
<td>Acme Packet 6300 Hardware Installation Guide</td>
<td>Contains information about the components and installation of the Acme Packet 6300.</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Contains information about the current documentation set release, including new features and management changes.</td>
</tr>
<tr>
<td>ACLI Configuration Guide</td>
<td>Contains information about the administration and software configuration of the Service Provider Oracle Communications Session Border Controller.</td>
</tr>
<tr>
<td>ACLI Reference Guide</td>
<td>Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.</td>
</tr>
<tr>
<td>Document Name</td>
<td>Document Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Maintenance and Troubleshooting Guide</td>
<td>Contains information about Oracle Communications Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.</td>
</tr>
<tr>
<td>MIB Reference Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Accounting Guide</td>
<td>Contains information about the Oracle Communications Session Border Controller’s accounting support, including details about RADIUS and Diameter accounting.</td>
</tr>
<tr>
<td>HDR Resource Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Administrative Security Essentials</td>
<td>Contains information about the Oracle Communications Session Border Controller’s support for its Administrative Security license.</td>
</tr>
<tr>
<td>Security Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Installation and Platform Preparation Guide</td>
<td>Contains information about upgrading system images and any pre-boot system provisioning.</td>
</tr>
<tr>
<td>Call Traffic Monitoring Guide</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Revision History

This section contains a revision history for this document.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2018</td>
<td>• Initial Release</td>
</tr>
<tr>
<td>March 2018</td>
<td>• Adds issue wherein an OCSBC downgrade allows for SIPREC operation on an inappropriate version</td>
</tr>
<tr>
<td>September 2018</td>
<td>• Adds &quot;Known Issues in S-Cz7.4.1M1&quot;.</td>
</tr>
<tr>
<td>December 2018</td>
<td>• Adds &quot;Deprecated Ciphers&quot;.</td>
</tr>
</tbody>
</table>
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 cannot 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>
<thead>
<tr>
<th>Boot flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000001</td>
<td>Disable all security filtering on all network interfaces</td>
</tr>
<tr>
<td>0x00000010</td>
<td>Enable direct Linux login on port 2200 via SSH for debugging</td>
</tr>
<tr>
<td>0x00000020</td>
<td>Enable the debug console</td>
</tr>
<tr>
<td>0x01000000</td>
<td>Enable SFTP access to protected files and directories</td>
</tr>
<tr>
<td>0x20000000</td>
<td>Enter failsafe mode</td>
</tr>
<tr>
<td>0x40000000</td>
<td>Boot directly to the Linux shell</td>
</tr>
</tbody>
</table>

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-----
   MIIEpAIBAAKCAQEAxd3bGH0tlLlaLmA35uveUbgRuoxqtiKSSn42rBKuRamaILO
   ++16Qn0kYVmCfxKpYhaQ3LCToer+/WRV4uVp5RNp4QR7UdMjhc8yxy22rHrW
   :.
   .
   tbNE27eOKBhLmd09WvU10qBumZmV+TtI87dEzn1T02J245mTEtJ3hWv00VhHh94t4
   Lyv/a8t/dV4+hvMFYC2Kh0ivJjAW6IPz6NhsK6qJhWReytL9CQ==
   -----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.
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
   ```

4. Save and activate your configuration

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

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/A8zrhhHxcLw6CBLGkAVSxw2jJBnBZNaYCd+L5gvJ1/eAYXqMww8yoL1cNIYVrd76DntnpvaGjcHoXjt00JD12ps6y2z02NJz2IznQtP
   ...
   ...
   mBD2P8icZ2Tw2GBfms3dktvA2QM4e4RhWQcyOtcee4Sw2E8HxzCvSM0h45ArEo
   jWzmx0dHaGis22F25kp/0N2D12rg1D2n5QaMoNPY+AOn0Dw0+F+
   -----END RSA PRIVATE KEY-----;
   ```
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.
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.

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.

Known Issues in S-Cz7.4.1M1

The following table lists S-Cz7.4.1M1 Known Issues.
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Found In</th>
<th>Fixed In</th>
</tr>
</thead>
<tbody>
<tr>
<td>28650852</td>
<td>The SBC changes the value of the P-Early-Media header in a 183 message to the sip-interface's <code>p-early-media-direction</code> parameter setting.</td>
<td>SCZ741m1</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

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