Unify OpenScape Session Border Controller V11

Release Notes

Software Version: V11 R3.4.1

Date 2026-07-02

☐ Major Release ☐ Minor Release ☐ Fix Release ☒ Hotfix Release

Includes Security Updates: Yes: ☒ No: ☐

Current release status can be verified via the Software Supply Server (SWS)

Deliverables
☒ Full Release ☐ Delta Release

Export Control Classification Data
AL: 5D002C1A ECCN: 5D002ENCR

Release Notes Version: V1.0

About this document

This document provides general information about the release, generics, and other relevant notes for the corresponding product and its correction versions.

NOTICE

OpenScape Session Border Controller
2026-07-03

Delivered Files

OpenScape Session Border Controller

Product Item Number		File Name
1	P30152-P1641-B1-20	image_oss-11.03.04.01-1.zip
	Zip file with: image_oss-11.03.04.01-1.tar – Software image file image_oss-11.03.04.01-1.spa – Software information file to use with CMP usbsticksetup_oss-11.03.04.01-1.zip – USB Stick Wizard	
2	P30152-P1641-B1-20	oss-11.03.04.01-1.bz2
	Software image for 4K Hosted	
3	P30152-P1641-B1-20	misc_oss-11.03.04.01-1.tar.gz
	Default XML configuration files and the MIBS	
4	P30152-P1641-B1-20	vApps_oss-11.03.04.01-1.zip
	OVF templates to create/deploy a virtual machine	
5	P30152-P1641-B1-20	sw-metadata-oss-11.03.04.01-1.json
	File used with OS Composer application	
6	P30152-P1641-B1-20	image_oss-11.03.04.01-1.ova
	OVA file to create/deploy a virtual machine	

Table of Contents

1. History of Change

1.1. Release Notes content

Version	Date	Description of changes
1.0	2026-07-03	OSSBC HotFix Release 11.03.04.01-1 – eeQA/Pilot Usage Updated item 1.2 – Product versions history Updated item 2.2 – Resolved Reported Problems / Symptoms

1.2. Product versions history

Software Version	Production Version	Date	Remarks
V11 R0.0.0	11.00.00.00-03	2023-10-09	
V11 R0.1.0	11.00.01.00-02	2023-10-30	
V11 R0.2.0	11.00.02.00-02	2024-01-02	
V11 R0.3.0	11.00.03.00-02	2024-02-26	
V11 R0.3.1	11.00.03.01-01	2024-03-01	
V11 R0.4.0	11.00.04.00-02	2024-04-15	Obsolete
V11 R0.5.0	11.00.05.00-02	2024-04-29	
V11 R0.6.0	11.00.06.00-02	2024-05-27	
V11 R0.6.1	11.00.06.02-01	2024-06-10	
V11 R0.6.2	11.00.06.02-01	2024-06-21	
V11 R1.0.0	11.01.00.00-03	2024-06-14	
V11 R1.0.1	11.01.00.01-01	2024-06-26	
V11 R1.0.2	11.01.00.02-01	2024-08-30	
V11 R1.1.0	11.01.01.00-01	2024-10-04	
V11 R1.1.1	11.01.01.01-01	2024-10-28	
V11 R1.1.2	11.01.01.02-01	2024-12-17	
V11 R2.0.0	11.02.00.00-02	2025-01-31	
V11 R2.0.1	11.02.00.01-01	2025-02-10	
V11 R2.1.0	11.02.01.00-01	2025-02-24	
V11 R2.1.1	11.02.01.01-01	2025-03-25	
V11 R2.2.0	11.02.02.00-3	2025-04-25	
V11 R2.2.1	11.02.02.01-1	2025-05-16	
V11 R2.2.2	11.02.02.02-1	2025-06-12	
V11 R2.3.0	11.02.03.00-2	2025-07-10	
V11 R2.4.0	11.02.04.00-1	2025-08-26	
V11 R3.0.0	11.03.00.00-4	2025-10-27	
V11 R3.1.0	11.03.01.00-1	2025-12-15	
V11 R3.1.1	11.03.01.01-1	2026-01-22	

V11 R3.2.0	11.03.02.00-2	2026-03-10	
V11 R3.3.0	11.03.03.00-1	2026-04-07	
V11 R3.4.0	11.03.04.00-1	2026-05-22	
V11 R3.4.1	11.03.04.01-1	2026-07-02	

Note: List of all software versions released since V11R0 software release in SWS

2. Changes

2.1. Implemented Change Requests / New features

Tracking Reference	Internal Reference	Summary	Released in Version
	OSSBC-12031	Dev - Update Opensuse 2023	V11 R0.0.0
	OSSBC-12857	Expand SBC Parameter ”Open external firewall pinhole”	V11 R0.0.0
	OSSBC-12021	Stand-alone BYOT for UO and MS Teams	V11 R0.0.0
	OSSBC-12412	SBC interworking with MS Teams Survivable Branch Appliance	V11 R0.0.0
	OSSBC-12219	Maintain OSB and SBC Custom HTTP PHP Scripts After Upgrade	V11 R0.0.0
		SIP Service Providers flags imported from OSB to SBC	V11 R0.0.0
		New V11 License Types	V11 R0.0.0
	OSSBC-12338	OS SBC released on OSB 550 and OSB 550HA hardware	V11 R0.0.0
	OSSBC-13749	Categorized Redundancy with different HW Pair Support	V11 R0.2.0
	OSSBC-5562	Support for TLS V1.3	V11 R1.0.0
	OSSBC-14130	OS SBC - Rebrand from Atos to Mitel	V11 R1.0.0
	OSSBC-14664	Allow user privilege escalation for ssh access over sudo	V11 R1.0.0
	OSSBC-13977	Add redundancy switchover button to the GUI	V11 R1.0.0
	OSSBC-14537	Force direction attribute to sendrcv	V11 R1.0.0
	OSSBC-11425	support Pidf-lo header as MSTeams for ELIN or be able to copy that info into PAI header PSR is required for this feature	V11 R1.0.0
	OSSBC-13678	MiVB/MX1 Mitel Products Integration with SBC	V11 R1.1.0
RQ00043371 / INC003389594	OSSBC-14913	Expand SBC Parameter ”Open external firewall pinhole” - Part 2	V11 R1.1.0
	OSSBC-15105	Create a repository for node apps and make them run standalone	V11 R1.1.0
	UIP-654	Validation of Mitel MiV5000 interworking with OpenScape SBC for MS Teams DR for SIP trunking	V11 R1.1.0
	OSSBC-15243	Log Viewer first programmed changes	V11 R1.1.0

Tracking Reference	Internal Reference	Summary	Released in Version
	OSSBC-14171	Update Opensuse 2024	V11 R2.0.0
	OSSBC-15063	Support OpenSSL 3.x	V11 R2.0.0
	OSSBC-13322	Add support for DNS NAPTR in sipserver	V11 R2.0.0
	OSSBC-15498	Block root user GUI access	V11 R2.0.0
	OSSBC-15499	VM deployment as OVA	V11 R2.0.0
	OSSBC-13861	Ability to classify traffic from MS Teams based on calling party to route to SITE trunks PSR is required for this feature	V11 R2.0.0
	OSSBC-14098	Dynamic registration with Hash Code and contact header in an option message	V11 R2.0.0
	OSSBC-15309	Zoom PSI remote SIP subscribers for standard SIP Clients working with OSV and OS4000	V11 R2.0.0
	OSSBC-15313	Inclusion of Cloud Link Daemon to support Zoom PSI	V11 R2.0.0
	OSSBC-15312	Zoom - Mobile push notifications	V11 R2.1.0
	OSSBC-5468	BNB-3182: SIPREC for Standard Enterprise Solutions for OS SBC to enable record all calls on trunk PSR is required for this feature	V11 R2.2.0
	OSSBC-15867	Dev - Homologate Lenovo SR250 V3, replacement for Lenovo SR250 V2 (OSB/SBC)	V11 R2.3.0
	OSSBC-15868	Dev - Homologate Lenovo SR630 V3, replacement for Lenovo SR630 V2	V11 R2.3.0
	OSSBC-16031	Second phase of Zoom support in OS SBC - Features TBD	V11 R2.3.0
	OSSBC-16219	Make Cloudlink to be whitelisted by default for Message Rate Control	V11 R2.3.0
	OSSBC-16218	Allow FQDNs to be Whitelisted for Message Rate Control	V11 R2.3.0
	OSSBC-16040	Configurable error code to Ip PBX for push notification failures	V11 R2.3.0
	OSSBC-16339	Configurable ciphers to SSH	V11 R2.4.0
	OSSBC-16340	Configurable ciphers to SIP-TLS	V11 R2.4.0
	OSSBC-16185	Update the July/August release of CLA and CLC software components that OS SBC and OSB uses	V11R2.4.0
	OSSBC-16122	Update OpenSUSE 2025	V11R3.0.0
	OSSBC-15513	OS SBC Header Manipulation Rules (HMR)	V11R3.0.0
	OSSBC-10531	SNMP event Too many subscribers registered and too many registered subscribers unreachable	V11R3.0.0
	OSSBC-16019	Security plan for product OS SBC V11.3	V11R3.0.0

Tracking Reference	Internal Reference	Summary	Released in Version
	OSSBC-16363	Allow OS SBC SIP Trunk creation in Workflow Studio	V11R3.1.0
	OSSBC-16489	Create option to not validate via headers for WFS	V11R3.1.0

Note: Additional info related to “Implemented Change Requests / New Features” Released in previous versions are available in the latest Release Notes for each respective version.

2.1.1. Update OpenSUSE 2025 (OSSBC-16122) [V11R3.0.0]

The operating system was upgraded to OpenSUSE Leap 16.0

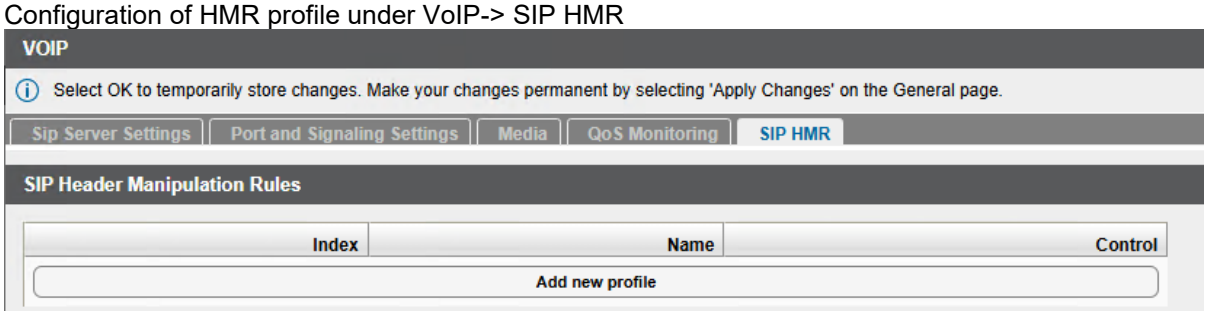
```
SBC-550-94:/home/administrator # cat /etc/os-release
NAME="openSUSE Leap"
VERSION="16.0"
ID="opensuse-leap"
ID_LIKE="suse opensuse"
VERSION_ID="16.0"
PRETTY_NAME="openSUSE"
ANSI_COLOR="0;32"
CPE_NAME="cpe:/o:opensuse:leap:16.0"
BUG_REPORT_URL="https://bugs.opensuse.org"
HOME_URL="https://www.opensuse.org/"
DOCUMENTATION_URL="https://en.opensuse.org/Portal:Leap"
LOGO="distributor-logo-Leap"
```

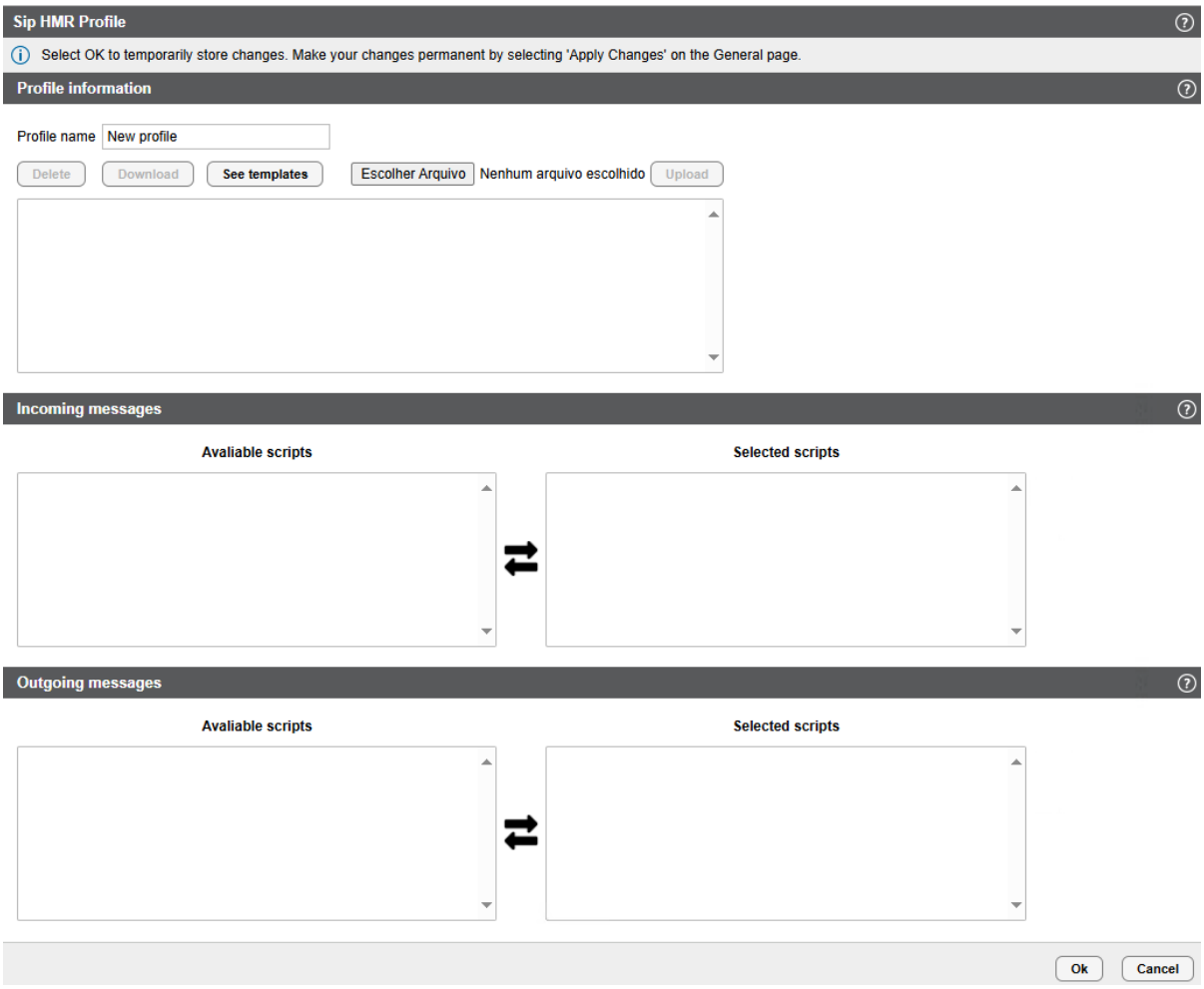
2.1.2. OS SBC Header Manipulation Rules (HMR) (OSSBC-15513) [V11R3.0.0]

Feature used to modify SIP Headers with use of Lua scripts.

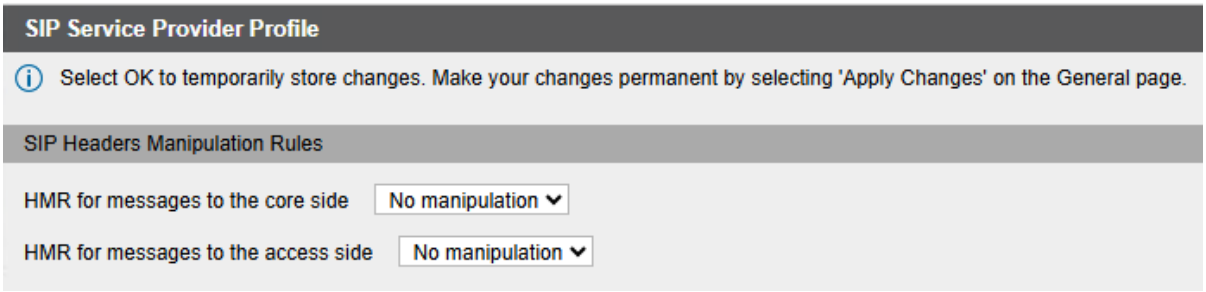
Can be applied to Remote Endpoint (Type as SSP) and Remote Subscribers.

Configuration of HMR profile under VoIP-> SIP HMR

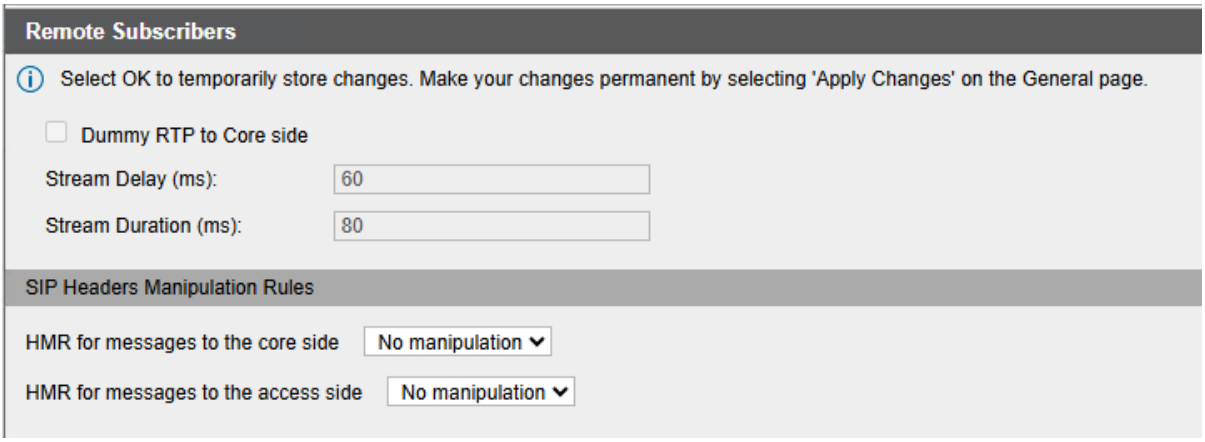




Association between HMR Profile and SIP Service Provider Profile



Association between HMR Profile and Remote Subscribers



For more detailed information, please check Online Help.

Important Notes:

- This feature can work alongside others, such as the SIP Service Address. When scripts are selected for Outgoing Messages, they take priority over the SIP Service Address, whereas for Incoming Messages, the SIP Service Address takes priority.
- Only .lua scripts can be uploaded.
- The uploaded scripts are not checked against Lua syntax. Therefore, it is the administrator's responsibility to check both the syntax and functionality of the scripts
- The pool is common for all HMRs, which means that one script can be used for multiple HMRs. If a script has a different behavior for a specific rule, it must be renamed and attached to that rule only; otherwise, it will affect all rules.
- It is possible to delete a script only if it is not being used in another profile.
- It is recommended to proceed with caution when modifying a selected template. The uploaded scripts are not checked against Lua syntax. Therefore, it is the administrator's responsibility to check both the syntax and functionality of the scripts.

Restrictions:

- Trying to remove and then add same header in the same direction either outgoing or incoming is not a valid use case.
- Different script name is required in case of reusing the same script.
- Wrong lua script will cause SBC malfunction after sip restart.
- In order to delete a selected lua script, unselect the script press ok and then go to profile and delete it
- Sometimes when download a Lua script name is changed

2.1.3. SNMP event Too many subscribers registered and too many registered subscribers unreachable (OSSBC-10531) [V11R3.0.0]

It´s an alarm for configuring a threshold for a minimum and maximum number of registered subscribers.

Configuration under Alarms->Alarm Settings

Group ID	Event ID	Group name	Event name	Active	Threshold	Trigger	Severity	Flow timer	Reporting class	Faulty object	Event type
6	2	Usage	Low number of registered users	☐	25	Less than	Critical	0	4	SIP Server	Communications
6	4	Usage	High number of registered users	☑	250	Greater than	Major	0	7	SIP Server	Communications

SNMP trap is sent when the alarm is generated.

Alarm “Low number of registered users” is disabled by default.

2.1.4. Security plan for product OS SBC V11.3 (OSSBC-16019) [V11R3.0.0]

Automatic Account Management for Inactive Users - BSR (Baseline Security Requirements)

Available from: V11R3

Administrators can now configure automatic security policies to lock and remove inactive user accounts after specified periods of inactivity.

Features:

Automatic Account Locking

- When creating an admin account, you can set a lockout period (in days)
- If a user doesn't log in within this configured timeframe, their account is automatically locked
- This helps maintain security by disabling accounts that are no longer actively used

Automatic Account Removal

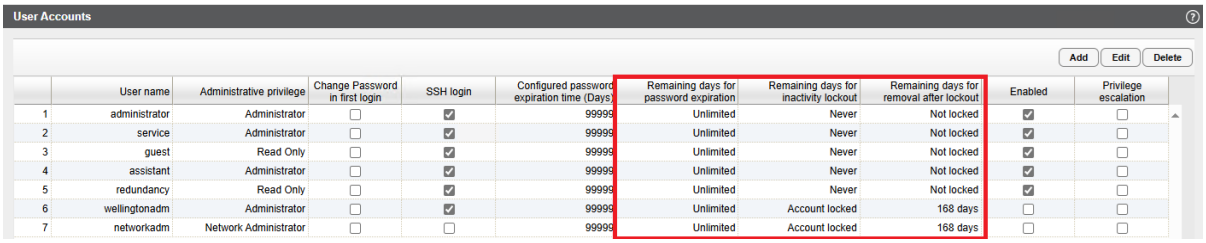
- You can also configure a removal period (in days) that begins after an account is locked due to inactivity
- If the locked account is not reactivated by an administrator within this removal period, it will be permanently deleted from the system
- This ensures that dormant accounts don't accumulate in the system

Monitoring:

You can view the time remaining until lockout and removal for any account on the **General Security** tab, allowing you to proactively manage accounts before they are automatically locked or removed.

Notes

- **Default users are exempt** from these automatic lockout and removal policies
- Locked accounts can be manually reactivated by an administrator at any time before the removal period expires

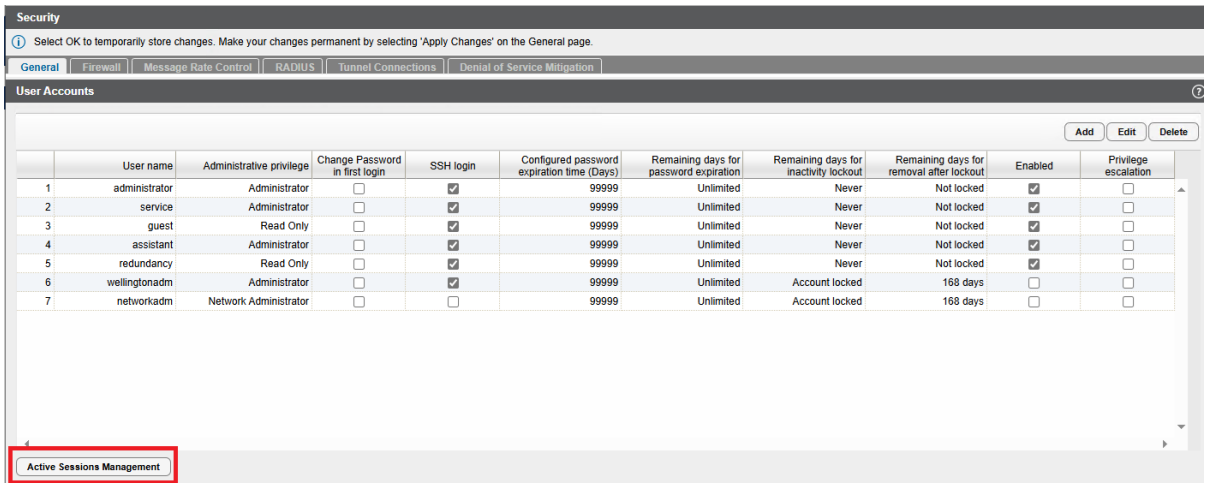


	User name	Administrative privilege	Change Password in first login	SSH login	Configured password expiration time (Days)	Remaining days for password expiration	Remaining days for inactivity lockout	Remaining days for removal after lockout	Enabled	Privilege escalation
1	administrator	Administrator	☐	☑	99999	Unlimited	Never	Not locked	☑	☐
2	service	Administrator	☐	☑	99999	Unlimited	Never	Not locked	☑	☐
3	guest	Read Only	☐	☑	99999	Unlimited	Never	Not locked	☑	☐
4	assistant	Administrator	☐	☑	99999	Unlimited	Never	Not locked	☑	☐
5	redundancy	Read Only	☐	☑	99999	Unlimited	Never	Not locked	☑	☐
6	wellingtonadm	Administrator	☐	☑	99999	Unlimited	Account locked	168 days	☐	☐
7	networkadm	Network Administrator	☐	☐	99999	Unlimited	Account locked	168 days	☐	☐

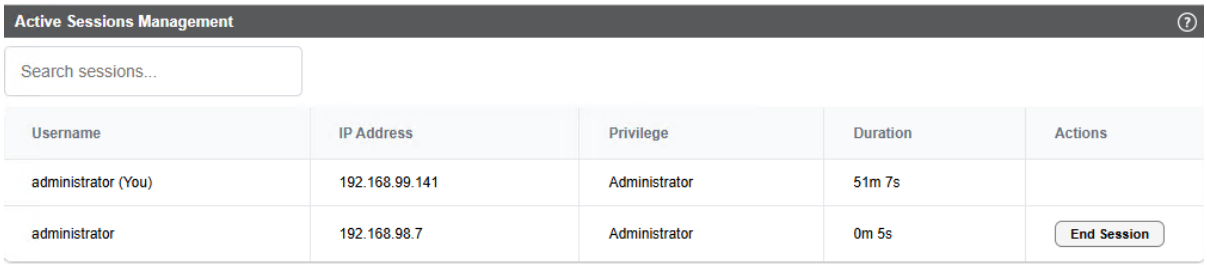
A new feature was also added to the same Security tab, this new feature is a button regarding to ticket OSSBC-15926 (Absence of Option to View and Logout From Active Sessions and Devices)

- Active sessions can be managed under the “Active Sessions Management“ button. The Active Sessions Management console provides an overview of all currently logged-in sessions, allowing you to review associated devices, timestamps, and terminate any session proactively.

All administrators have access to the feature, but they can only view sessions of users with privileges equal to or below their own.



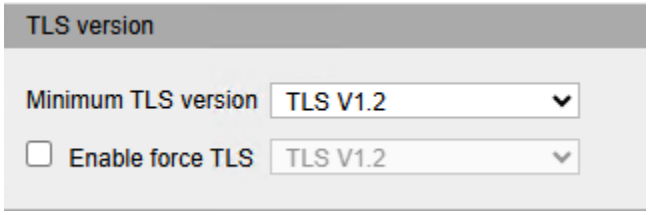
When clicked on the “Active Sessions Management” this is the window that is opened:



2.1.5. Certificate Profile – Force TLS version (OSSBC-16453) [V11R3.0.0]

When enabled, this option enforces the use of a specific TLS version for the connection. After enabling the flag, you can select the desired TLS version in the adjacent field.

Configuration under: Security -> General -> Certificate management -> Certificate profile -> TLS version



This option is currently available only for SIP-TLS certificates.

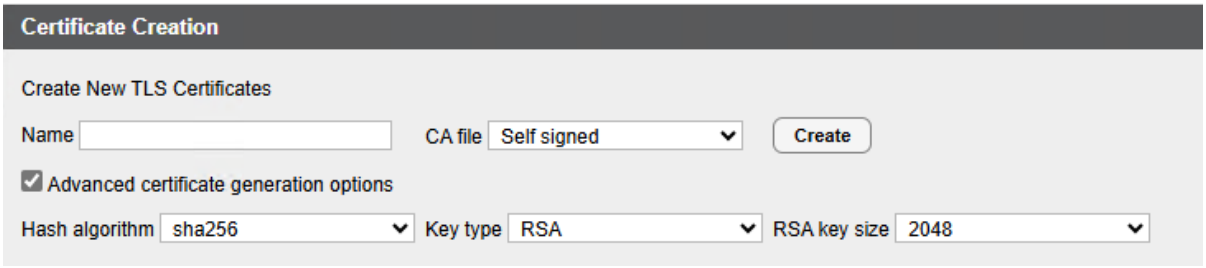
2.1.6. System´s default DTLS version to 1.2 [V11R3.0.0]

Starting from the V11R3 now the default is DTLS 1.2 for all the system, even though a DTLS profile is not configured.

2.1.7. Advanced option when creating a new TLS Certificate [V11R3.0.0]

Starting from the V11R3, it is possible to create a new TLS certificate with advanced options. It is now possible to select a specific Hash Algorithm, Key Type and RSA Key size.

This option is disabled by default.

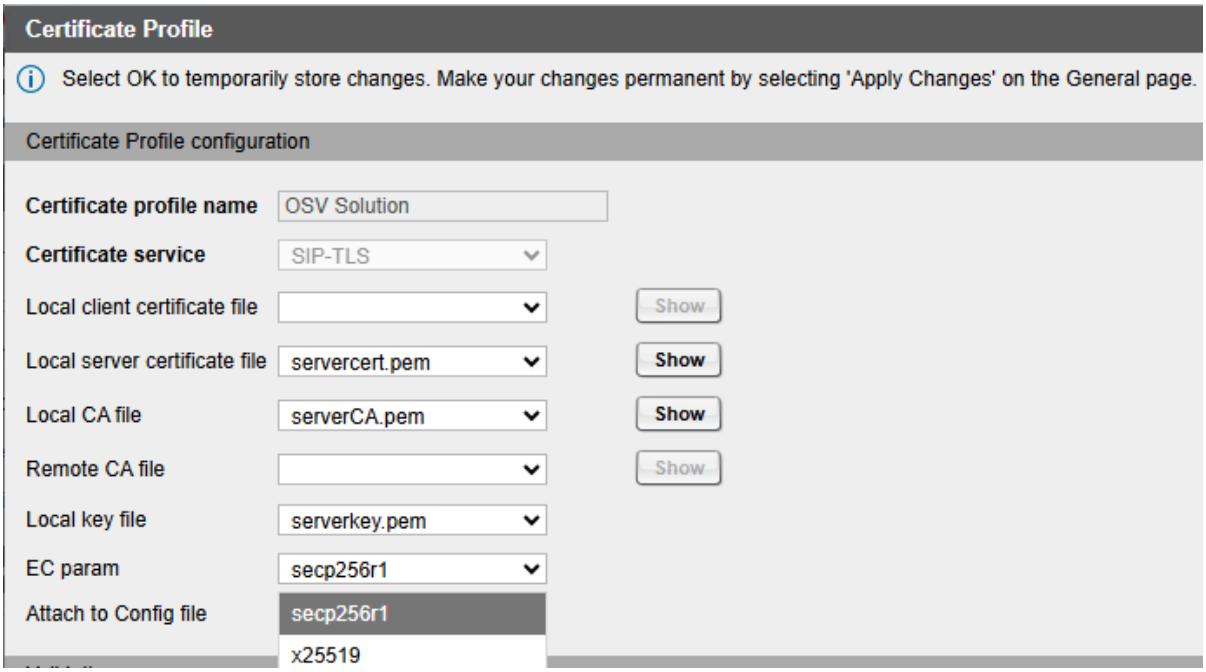


NOTE: Creating a weaker certificate may compromise security

2.1.8. TLS 1.3 Connection with OSV V11 [V11R3.0.0]

Starting from version V11R3, the default SIP connection with the OSV continues to use the secp256r1 elliptic curve from the OSB and OSSBC side to ensure compatibility with OSV V11. This configuration was retained as secp256r1 because OSV V11 does not support the X25519 curve, which is the default in newer OpenSSL versions.

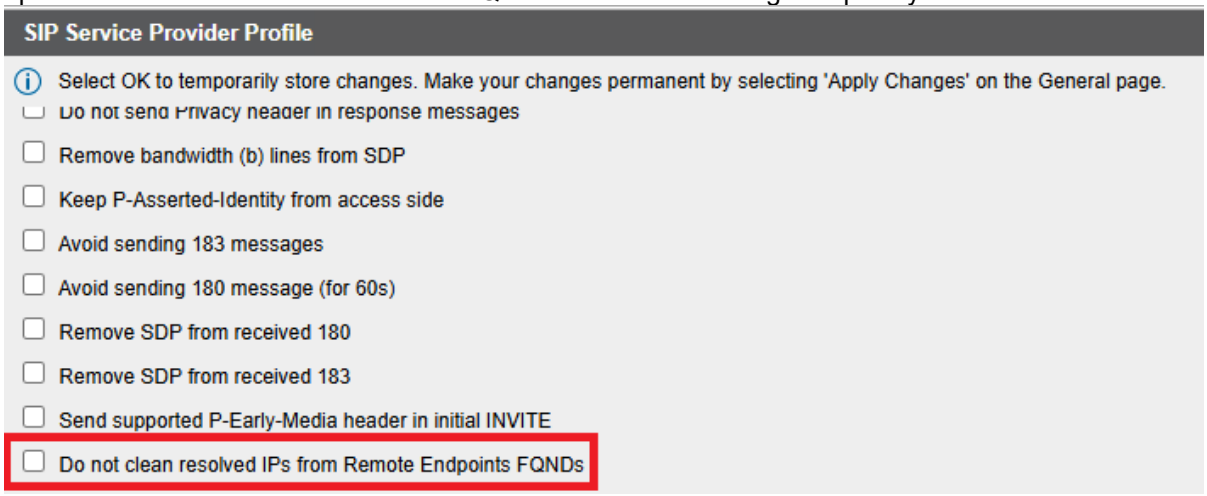
NOTE: It is also possible to configure the EC Param



2.1.9. Create a flag in the SSP Profile to never cleanup resolved FQDN addresses

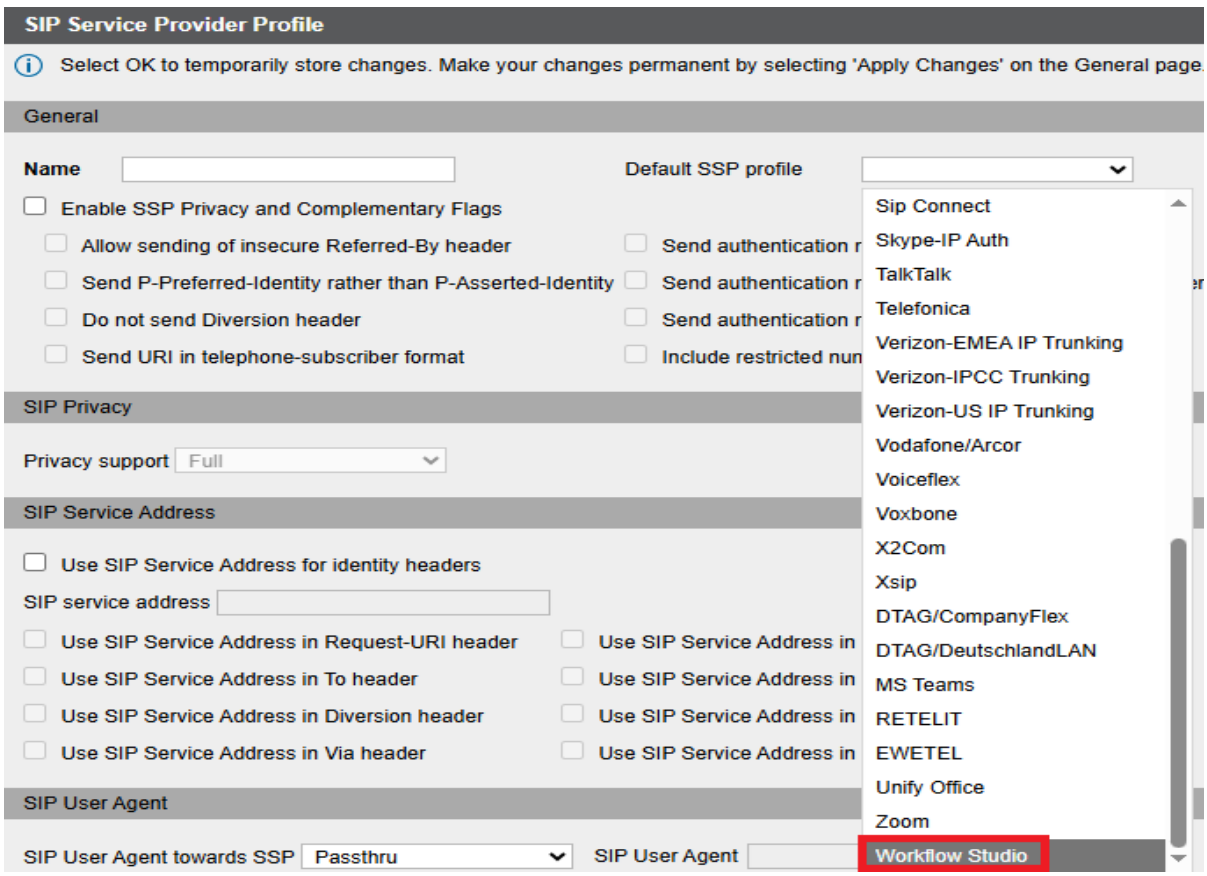
(OSSBC-16373) [V11R3.0.0]

If set, the SBC will retain the resolved IP addresses of the associated Remote Endpoint FQDNs. This option is useful in scenarios where the FQDN IP addresses change frequently.



2.1.10. Allow OS SBC SIP Trunk creation in Workflow Studio (OSSBC-16363) [V11R3.1.0]

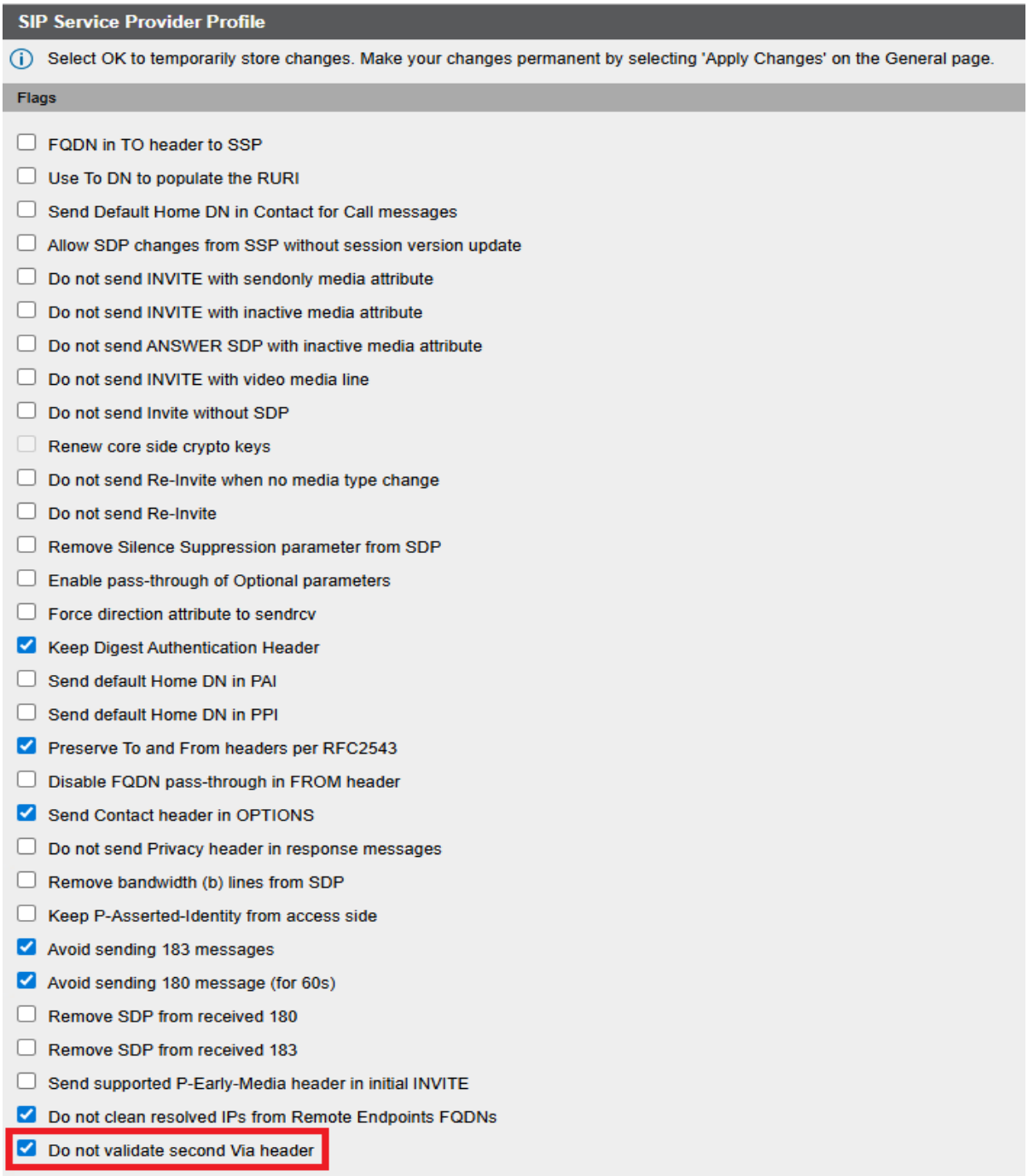
New “Default SSP Profile” available -> Workflow Studio



2.1.11. Create option to not validate via headers for WFS (OSSBC-16489) [V11R3.1.0]

New flag available under SIP Service Provider Profile -> “Do not validate second Via header”

When enabled, the SIP server skips verification of the second Via header. This validation is typically performed when an SSP is located behind the outbound proxy. When this option is enabled, only the outbound proxy address is validated



2.1.12. Push Notification for VoIP requires update (2026) (OSSBC-16727) [V11R3.3.0]

The OpenScape Mobile Push Certificate for APN will expire on **May 4th ,2026** and requires to be updated in the SBC, otherwise, delivery of push notification for APN Server will not be possible. The Default IOS Push certificate profile needs to update using the new certificate valid for 12 months.

The new certificate will be delivered starting from SBC build V11R3.3.0.

The new certificate is also available as attachment (SWS) in this release (V11R3.3.0).

If customer does not want to update to this build, it is possible to add the certificate OSMO_Pro_VoIP_APN_cert_2027.p12 manually via SBC Local GUI.

NOTE: the “IOS Push Default” certificate profile is locked to edit and the new way to use another certificate for IOS is to create a new profile.

1 - Enter in Security folder, General/Certificate Management

2 - Add the new certificate. Choose Certificate Upload, Key Files. Select the new file in Upload key file and press Upload. Confirm the file in Key files.

3 - In Certificate Profiles, add a new Profile with “Certificate service” as “IOS Push” and selects the new certificate file in Local key file. Press OK.

4 - Press OK again to close the Certificate Management folder.

5 - Press OK to close the Security folder.

6 – Select this new profile under “IOS Push certificate profile”

7 – Apply Changes

NOTE: The IOS Push certificate will be updated automatically only when the previous certificate is configured in certificate profile "IOS Push Default" .
For example: if the current certificate is OSMO_Pro_VoIP_APN_cert_2026.p12, after upgrade to V11R3.3.0 it will be automatically replaced by OSMO_Pro_VoIP_APN_cert_2027.p12 certificate, when in use on profile "IOS Push Default".
If the OSMO_Pro_VoIP_APN_cert_2026.p12 certificate is used in another IOS Push certificate profile, it will not be updated automatically. In such case, it is mandatory to edit the certificate profile and manually change this certificate to the new OSMO_Pro_VoIP_APN_cert_2027.p12 certificate (in “Local Key file” column) and Apply Changes.

2.2. Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary	Released in Version
	OSSBC-16824	Hyper-V - Additional network interfaces are not available on Local GUI (only in linux)	V11R3.4.1
PRB000293759	OSSBC-16798	Problem with incoming calls after upgrade from V11R1.0.0 to V11R3.4.0	V11R3.4.1
	OSSBC-16795	Change text under command "rmc status" to avoid confusion with mastership in redundancy mode	V11R3.4.1
	OSSBC-16794	Opensuse Leap 16.0 Update Cycle 2026-5	V11R3.4.1
PRB000291178	OSSBC-16783	Sporadically SBC does not process the first Incoming Invite from MS teams due to failed DNS resolver	V11R3.4.1
PRB000290584	OSSBC-16781	SBC V11R3.3.0 Memory 100%	V11R3.4.1
PRB000278163	OSSBC-16752	No RTP after 30 minutes	V11R3.4.1
	OSSBC-16776	CVE-2026-46300: Linux Kernel "Fragnesia" Local Privilege Escalation	V11R3.4.0
	OSSBC-16774	PRB000290925: CVE-2026-43284, 43500: OSSBC- Linux Kernel "Dirty Frag" Local Privilege Escalation	V11R3.4.0
PRB000290080	OSSBC-16772	The SSM process on SBC V11 R3.3.0 restarted unexpectedly, generating a coredump.	V11R3.4.0
PRB000290176	OSSBC-16771	it is not possible to refresh license from license server if you are connected with FQDN to SBC cluster	V11R3.4.0
PRB000290044, PRB000290016	OSSBC-16768	CVE-2026-31431 Local Privilege Escalation in Linux Kernels	V11R3.4.0
	OSSBC-16767	Opensuse Leap 16.0 Update Cycle 2026-4	V11R3.4.0
PRB000285296	OSSBC-16765	SBC receives SDP with payload type 101 from Core side but does not forward it to access side although configured	V11R3.4.0
PRB000289877	OSSBC-17764	Frequent call drops on the Genesys Cloud CX	V11R3.4.0
PRB000288901	OSSBC-16760	Core Realm port validation for SBC in Standalone mode (V11 R3.XX.XX).	V11R3.4.0
PRB000288514	OSSBC-16759	Incorrect SIP ACK Header Mapping (Topology Hiding Failure)	V11R3.4.0
PRB000286712, PRB000288387	OSSBC-16751	Deleting one of the route prefixes from Remote endpoint configuration triggers loss of Remote Endpoint configuration	V11R3.4.0
PRB000281485	OSSBC-16687	Inbound DTMF intermittent failure	V11R3.4.0

The resolved problems in this release and in the previous releases are listed in the spreadsheet:

OpenScape_SBC_V11R3.4.1_Resolved_Problems_And_CVEs_V1.0.xlsx
See chapter 8 “References” for its location.

2.3. Resolved Vulnerabilities

Tracking Reference	Internal Reference	Severity Level	Summary	Released in Version
CVE-2026-46300	OSSBC-16776	High	CVE-2026-46300: Linux Kernel "Fragnesia" Local Privilege Escalation	V11R3.4.0
CVE-2026-43284, 43500	OSSBC-16774	High	PRB000290925: CVE-2026-43284, 43500: OSSBC- Linux Kernel "Dirty Frag" Local Privilege Escalation	V11R3.4.0
CVE-2026-31431	OSSBC-16768	High	CVE-2026-31431 Local Privilege Escalation in Linux Kernels	V11R3.4.0

The resolved vulnerabilities in this release and in the previous releases are listed in the spreadsheet (tickets marked with “Yes” in the “Security Relevant” column or for all the solved vulnerabilities, can be checked in the tab “CVEs” in the spreadsheet):

OpenScape_SBC_V11R3.4.1_Resolved_Problems_And_CVEs_V1.0.xlsx

See chapter 8 “References” for its location.

Note: It is strongly recommended applying this fix version if it includes resolved vulnerabilities.

2.3.1. Vulnerability Impact Evaluations

Tracking Reference	Internal Reference	Reported Severity Level	Mitel Assessment Severity Level	Summary
CVE-2026-46300	OSSBC-16776	High	High	CVE-2026-46300: Linux Kernel "Fragnesia" Local Privilege Escalation
CVE-2026-43284, 43500	OSSBC-16774	High	High	PRB000290925: CVE-2026-43284, 43500: OSSBC- Linux Kernel "Dirty Frag" Local Privilege Escalation
CVE-2026-31431	OSSBC-16768	High	High	CVE-2026-31431 Local Privilege Escalation in Linux Kernels

3. Important Issues, Workarounds, Hints and Restrictions

This section provides the latest information at time of software release and is only pertaining to the time of release notes generation.

3.1. Important Issues

3.1.1. Custom DNS files

Using Custom DNS files in V11R2, it is necessary to specify the directory "/var/lib/named" in named.conf file.

options

{ directory "/var/lib/named"; }

In previous version, in named.conf file, it was not specified.
options {
};

See the link https://doc.opensuse.org/documentation/leap/reference/html/book-reference/cha-dns.html# related to The domain name applied to openSUSE Leap 15.4.

NOTE: If Custom DNS files are already used in previous release, for example running V10R2, it is recommended to change the named.conf before the upgrade to V11R2.

NOTE: Please verify that the line inside of the DNS file is written as " file root.hint " rather than " file root.hints " . If it is already correct, no modification is required:

```
zone "." {
        type hint;
        file "root.hint";
}
```

3.1.2. OpenScape SBC is affected by a deprecation of a legacy Firebase API (OSSBC-14806)

This API is used for push notifications of Android calls to OSMO, and its interface will be removed on **September 20, 2024.**
The mobile application will not be notified to wake up when running in the background preventing the SIP phone from receiving any notification, including incoming calls.

When in the foreground, the client will behave normally.

A permanent solution is provided in this release.

3.1.3. TLS Client Hello Handshake fails between CMP and SBC (OSSBC-14924)

Communication between CMP and OSSBC is broken if TLS 1.0 is configured in the https certificate profile.

As workaround change the parameter "Minimum TLS version" to TLS V1.2 for HTTPS certificate profile before upgrade the system to V11R1.

3.1.4. Error after fix for FCM new API when OSMO in background (OSSBC-14873)

PRB000077241: Intermittently OSMO Android devices cannot be called after updating OSSBC to V11 R1.0.0.

This issue was fixed on previous releases.

3.1.5. tel uri in requests to OSV/4k since V11R2.1.0 (OSSBC-16047)

Due to a recent fix, a change was implemented using an internal control variable of the SIP Server core, as per the component documentation. This variable ended up exposing a usage problem within this OpenSource component. As a result, SIP call headers ended up being replaced by tel-uri. Depending on the scenario and the IP-PBX, this change could either go unnoticed or cause other side effects such as uncompleted calls, dropped calls, audio problems, among others.

A permanent solution was fixed on previous releases.

3.1.6. Redundancy issues (OSSBC-16131 and OSSBC-16138)

Due to the following issues detected on redundancy systems:

OSSBC-16131 (PRB000084343) – Virtual IP added at WAN side (access side) is wrong, causing e.g calls and registration error. This is happening on systems that have additional network interfaces configured at access side.

OSSBC-16138 (PRB000084367) – System upgrade is not working when the flag "Enable access link connectivity check" is enabled.

The recommendation for customers that have redundancy systems **DO NOT UPGRADE to V11R2.2.0.**

A permanent solution is included on V11R2.2.1 and higher versions.

3.2. Workarounds, Hints

3.2.1. Workarounds

3.2.1.1. CloudLink Server download failure

Before performing a local file upgrade, place the IP address of the server where the new software image is into the Message Rate Control White List.

Identify the IPs with the command:

nslookup download.mitel.io

Then add the IPs listed to whitelist as follows:

Via SBC LOCAL GUI → Security → Message Rate Control → White List → type IP addresses and click "Add" and "Apply Changes"

3.2.1.2. Administrative and redundant connections are timed out after upgrading a redundant SBC (OSSBC-16614)

After upgrading to V11R3, in some systems, Local GUI and ssh connection were not accessible due to timeouts.

If the issue occurs, as workaround, please reboot the node.

Non-redundant system may possibly be affected by this issue.

Note: this issue is fixed on this HotFix (V11R3.1.1)

3.2.1.3. After upgrade at V11R3.0.0 access through CMP fails with error 403 (OSSBC-16630)

After update of the OSSBC/OSB to V11R3.0.x and onward it's not possible to configure the SBC or OSB via the CMP.

As a Workaround, please connect directly through OSSBC/OSB via Local GUI interface.

Note: this issue is fixed on this HotFix (V11R3.1.1)

3.2.2. Hints

3.2.2.1. Deprecated Linux Networking Commands

In V11, the deprecated linux networking commands arp, ifconfig, netstat and route, were replaced by:

Linux Deprecated Commands	Linux Replacement Commands
arp	ip n (ip neighbor)
ifconfig	ip a (ip addr)
netstat	ss
route	ip r (ip route)

3.2.2.2. Firewall Considerations in Single-Armed installation

In Single-Armed installation, it is necessary to add the private IP address subnet used by the customer to the Firewall Whitelist in order to allow access to the SBC GUI from that subnet.

The reason this is needed is because the SBC blocks private subnets that are not in its own subnet.

One important information is that during the installation process over usb-stick the firewall rules are not applied yet and thus, at that moment a user will have access to the SBC, even if they are in a subnet that would be blocked later when the system starts up after the installation was completed.

One way to avoid being locked out is to add the desire subnet to the Firewall whitelist during the usb-stick operation, apply changes before finishing the installation.

In cases where the auto-install option is desired, a pre-set database with the subnet configured in the Firewall whitelist will be required to prepare the usb-stick iso image.

3.2.2.3. TLS Certificate alarms

If the TLS certificate out of validity or TLS certificate expired alarms are shown, please verify if the https and service_api default certificate are not expired.
They use https default certificate. This certificate expires after two years after first installation.

See in Certificate Management, Certificate Profile, certificate file Show button.
To solve it, create the new certificate in Certificate creation. For example, use the self-signed option.
After that create the new certificate profile for https and service api using the new certificates.
Change the system certificate profile related to HTTPS and SERVICE API to these new certificate profiles.

Note: In previous version, these alarms were not shown. It was corrected.
After full install using the new version, these alarms are not shown.

3.2.2.4. Dialogic SBC (OSSBC-12996)

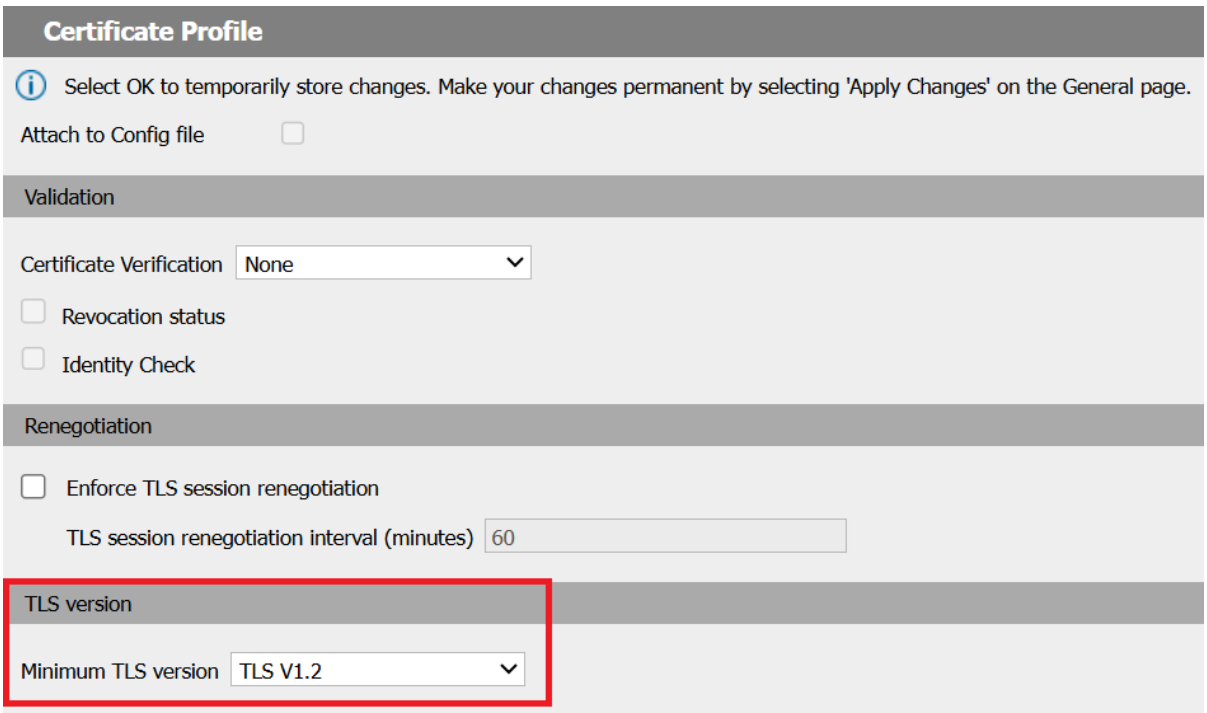
When Dialogic SBC is used and reinvite is sent to SBC, the SSP profile should have the "Do not send Re-Invite" enabled.

And Media Profile should have the option "Support ICE" disabled.

3.2.2.5. Certificate Profile – Minimum TLS Version

Recommendation is to configure the Minimum TLS version to be supported as v1.2.

This configuration is performed under: Security -> General -> Certificate management -> Certificate profile -> TLS version, selecting the option “TLS V1.2”



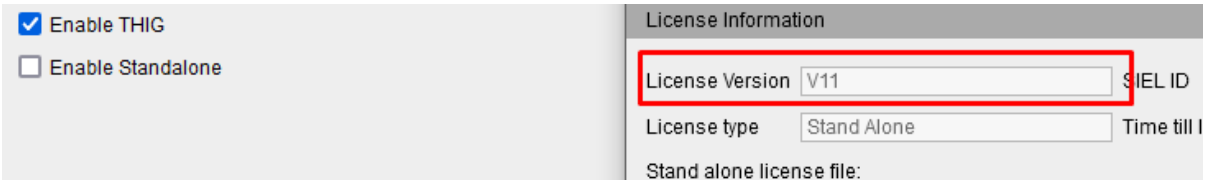
3.2.2.6. THIG License V11

In older V11 versions of the software some systems could have found a problem if a V9 or a V10 license with THIG was being used. An alarm would show about not having “SBC Sessions” in the license.

Other problem was that, if a system with THIG feature was updated to the V11R1, the feature would be disabled and should be enabled manually.

For both problems to be solved, the feature **THIG** was re-introduced in this Fix Release (V11R1.1.0)

Now is possible to use, without any problem, the THIG feature after an upgrade if the system has a V9 license or V10 license with "**THIG**" or if the system has an V11 license with "**SBC sessions**".

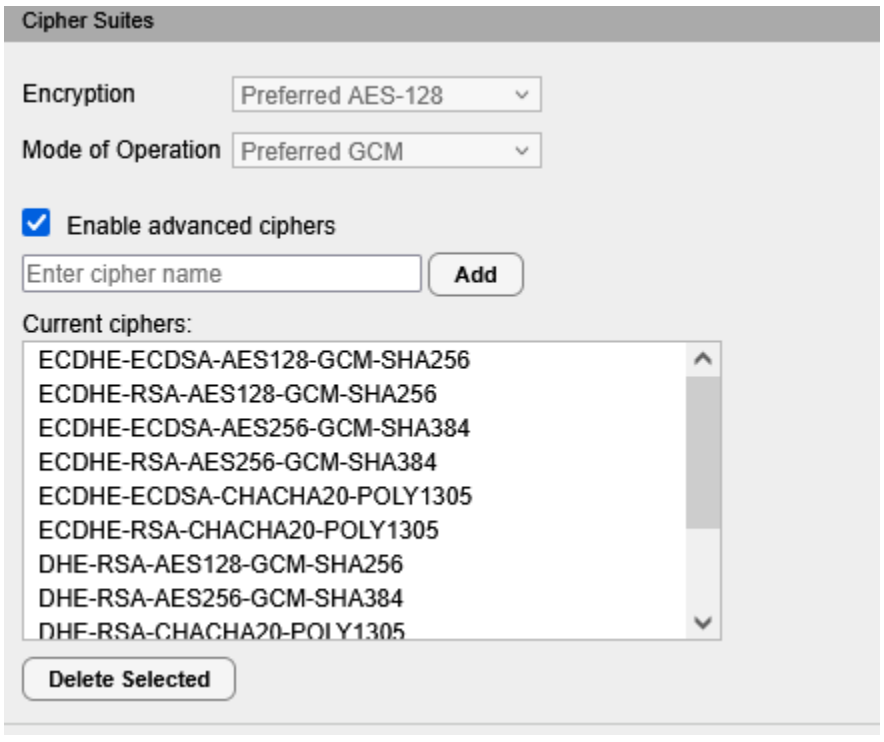


The feature can be enabled under:

Features > Enable THIG

3.2.2.7. Deprecated Ciphers – Configurable Ciphers (OSSBC-15917)

Starting from V11R2.3.0, deprecated cipher suites have been removed from the HTTPS default configuration, an advanced cipher option was introduced to give users more flexibility if they need to enable specific ciphers.



It is possible only to select and add ciphers when creating a new HTTPs certificate. Default HTTPs certificate is not configurable.

3.2.2.8. MS adapter does not accept requests from the OSB second MGCP IP (OSSBC-16232)

With this implementation, it is aso required to add the CCM IPs in the Trusted List.

3.2.2.9. Registration problems from Fusion users (OSSBC-16213)

Starting from the V11R2.4.0 a new field was added.

This field will define the number of allowed tcp connections from the same source IP. Default value is 1024.

Security > Deniel of Service

3.2.2.10. Activating the feature “Open External Firewall Pinhole”

It is recommended to proceed with caution when activating the feature “Open External Firewall Pinhole”. Be absolutely certain that the feature is necessary; otherwise, activating it can affect the media path and cause unexpected results in some environments. Additionally, the flag “Dummy RTP to Core side” should be avoided.

3.3. Restrictions

3.3.1. Restrictions or Exceptions for this current release

3.3.1.1. General

- The Local GUI is optimized for current versions of Chrome, Edge and Firefox. Please note that using IE or other browsers may lead to rendering errors and/or limited functionality.
- When the flags “Do not send Invite without SDP” and “Do not send Re-Invite” are being used in SSP Profile, we have the following restriction:

There is a restriction to use Mikey and DTLS in Media Profile (core and access side) when these flags are being used.

If Mikey or DTLS are configured in media profile, the invalid configuration message is shown in GUI during Apply Changes.

The recommended migration path is to move the configuration from MIKEY to SDES.

Restrictions Related to New V11 Features:

- When parameter "Comm System Type" under Sip Server Settings is configured as "Standalone with Internal SIP Stack" (BYOT mode), transfers of calls received from the SSP/PSTN by a MS Teams/UO user will not work with method REFER. But INVITE with Replaces header works.

3.3.2. DNS Server used by V11 must support the EDNS feature.

The Extend DNS feature allow the DNS servers to exchange messages greater than 512 bytes and this is now a request in V11 system.

The big packages will allow a better performance of the DNS servers. It is very easy to disable and enable EDNS on Windows Server 2008 R2 or later.

Statistics say that 85% of DNS servers already use EDNS, so do not disable EDNS on the DNS Server.

DNS server should also support EDNS COOKIE in received DNS queries.

In case the DNS Server does not support this, it should be configured to ignore EDNS COOKIE or DNS Server should be updated in a newer version that will support EDNS COOKIE. Otherwise, DNS Server may respond "*Format Error"* or similar error.

3.3.3. Validation of Mitel MiV5000 interworking with OpenScape SBC for MS Teams DR for SIP trunking (UIP-654).

The SBC transcoding feature is not released when integrated with the MiV5000 and therefore it cannot be activated in this configuration.

This is currently planned for a future OSSBC release.

4. Installation and Upgrade / Update

4.1. Installation

To unzip the SBC_SOFTWARE_PACKAGE.zip, use WinZip or 7zip, **do not use WinRAR**.

A full Installation erases both backup and active partitions and overwrites them with software from the USB drive.
A USB drive is required for this procedure.
To perform a full installation, please follow these steps:

- Create a USB stick using the provided utility and enter the network information for the server
- Make sure that the WAN address is configured when the USB stick is created
- Plug the USB stick into the OpenScape SBC server and reboot the server.
  Ensure the server is connected to the network
- The server will boot from USB and will become online.
- Using a web browser access the local management tool and start the installation process from the "Maintenance **->** Install/Upgrade" tab.
- User will be prompted when to remove the USB stick and a message will inform about a successful installation and final restart.
- After the restart the system will be up and running.
  It will take about 10 minutes after the restart for the system to perform a self-diagnosis.

NOTE: For a detailed description of the above installation procedures please refer to the "OpenScape SBC Configuration Guide".

NOTE: If an existing SBC is to be re-installed with USB stick or ISO image and this SBC used non-default TLS certificates and certificate authority files, these files should be saved from the existing SBC to a safe place and re-applied after the installation.
The files are located on the SBC in **/etc/openbranch/ssl/certs/vpn** folder and subfolders.
If these files are referenced in any certificate profiles and the XML of the SBC is exported and reused, then this XML configuration cannot be saved on the new installation until the matching certificate files are uploaded as well.

NOTE: In new installation, there is a new option to select the number of code partitions to be created.
The default is 2 (one for the active version and other for the backup version).
From now, it is possible to have until 5 partitions of code.
Despite the number of partitions selected, the number created can be below due to the disk size limitations.
For instance: you can select 5, but just 3 will be created.

NOTE: The RAID Controller() is configured to RAID1 in order to install OSB/SBC software for RX200, 3550 and SR530.
Please refer to chapter 3 to the following document for instructions: OpenScape Voice V10, Service Manual: Installation and Upgrades, Installation Guide

4.1.1. Data and Information Security

It is mandatory to apply the Security Checklist so that system default settings are hardened according to best practices. This is most relevant after a first installation, but also strongly recommended after each Major or Minor version upgrade. It presents a checklist to ensure all necessary installation and configuration steps can be taken and adapted to the individual customer's environment and security policy. Deviations from the standard settings should be documented in the security checklist in consultation with the customer's contact person.

The best possible standard of data security and protection is only provided on our latest solutions or product versions. It is recommended to regularly install product updates in order to remove identified security vulnerabilities and software defects, improve stability and add latest functionality.

Country-specific regulations must be observed.

The latest version of "OpenScape Session Border Controller V11 Security Checklist" can be found here.

4.2. Upgrade / Update / Migration

For more details on how to upgrade, refer to the upgrade section in the "OpenScape SBC Configuration Guide".

Current SW version	Upgrade Method-Intermediate Step	Upgrade Method-Final Step	New version
V11R3.x.x	-	Upgrade to V11R3	11.03.04.01-1
V11R2.4.0	-	Upgrade to V11R3	11.03.04.01-1
V11R1.1.2	-	Upgrade to V11R3	11.03.04.01-1
V11R0.6.2	-	Upgrade to V11R3	11.03.04.01-1
V10R3.6.1	-	Upgrade to V11R3	11.03.04.01-1
V10R2.6.1	-	Upgrade to V11R3	11.03.04.01-1
V10R1.5.2	-	Upgrade to V11R3	11.03.04.01-1
V10R0.5.4	-	Upgrade to V11R3	11.03.04.01-1
Equal or Higher than 09.04.12.X	-	Upgrade to V11R3	11.03.04.01-1
Lower than 09.04.12.X	First Upgrade to 09.04.12.X	Second Upgrade to V11R3	11.03.04.01-1
08.01.13.00-1	First Upgrade to 09.04.12.X	Second Upgrade to V11R3	11.03.04.01-1
07.01.33.01	Fresh install w/ existing db	-	11.03.04.01-1
02.00.32.006	Fresh install w/ existing db	-	11.03.04.01-1

NOTE1:

Direct upgrade to V11R3 is allowed ONLY when OpenScape SBC system is running with V9R4.12.X or higher.

NOTE2:

It is recommended to upgrade (local file upgrade to the latest version of the current SBC software release (listed above, leftmost column) before upgrading to a new SBC software release (i.e. from V9 to V10) using the upgrade method in the table above.

The Direct Upgrade/Upgrades from earlier V8R1 and V9 version not listed above are not supported and it is necessary to follow the steps in Note1.

In case of update/upgrade failures, fallback to the backup partition and apply the recommended/tested upgrade path as stated above.

For V10R0 Release, the direct upgrade to V11R3 is allowed when SBC system is running with V10R0.5.4 or higher.

NOTE3:

When upgrading OSBs or OS-SBC units to V10, the centralized OSB/OS-SBC license file needs to reflect the entire OSB/OS-SBC network and not just and individual OSB/OS-SBC that is being upgraded.

NOTE4:

Before performing a local file upgrade, place the IP address of the server where the new software image is into the **Message Rate Control White List**.

Via SBC LOCAL GUI → Security → **Message Rate Control White List** → type IP address and click "Add" and "Apply Changes".

NOTE5:

Please check the OpenScape Applications release notes to validate the compatibility between the product version of the centralized OpenScape Branch/SBC license file and the OpenScape Branch/SBC Assistants.

Do not import a centralized OpenScape Branch/SBC license with a higher product version as indicated in the OpenScape Applications release notes as this may activate immediate license enforcement of OSB/OS-SBC units.

The product version of a centralized license is usually included in the license file name or can be found in the "product" section of the license file.

Example based on a license file name of a centralized OpenScape Branch/SBC license …

ALI_or_MAC_of_CMP_OpenScape_Branch_SBC_**V10**.lic

… or based on the "product" section of the license file

…

<product>

<id>OSB</id>

<name>OpenScape Branch/SBC V10</name>

<version>**V10**</version>

<description>

<text lang="EN">OpenScape Branch/SBC V10</text>

</description>

<validity days/>

</product>

…

OSB/OS-SBC units running on a higher product version then included in the centralized OpenScape Branch/SBC license file are backward compatible to overcome intermittent combinations that may result during solution upgrade scenarios.

However, licensed features implemented in higher product versions will not work with a centralized OpenScape Branch/SBC license file from previous product versions.

NOTE6:

Starting from V10R2.3.0, it will implement check for M44 (end of life date) field and updates/upgrades are not allowed after this date. If the system is using a license with M44 status, the update/upgrade is not allowed. Then, it is necessary the extended support for the license with M44 status or a license with M3 status. The system will try to alert the user about this limitation as soon as possible. The system accepts V9 or higher licenses (V9 is already in M44 although the blockage isn´t currently enforced).

If the license version field is empty, the update/upgrade will not be allowed. In this case, please apply the supported license again and check license version before the update/upgrade.

NOTE7:

For Virtual Machines, the memory size was changed from V10R1.

OSS-250	OSS-6000	OSS-20000
4Gb	4Gb	6Gb

NOTE: PLEASE, CHANGE THE MEMORY IN VM BEFORE TO UPGRADE TO V11R0.

4.2.1. Fallback

If the check of installation fails, the system will reboot to backup partition. In case of a full installation and both partitions are failing then a re-installation using same procedure is required.

If a regular upgrade was done, Backup Partition containing previous version can be restored using Local GUI → Maintenance → Restart → Restart to backup.

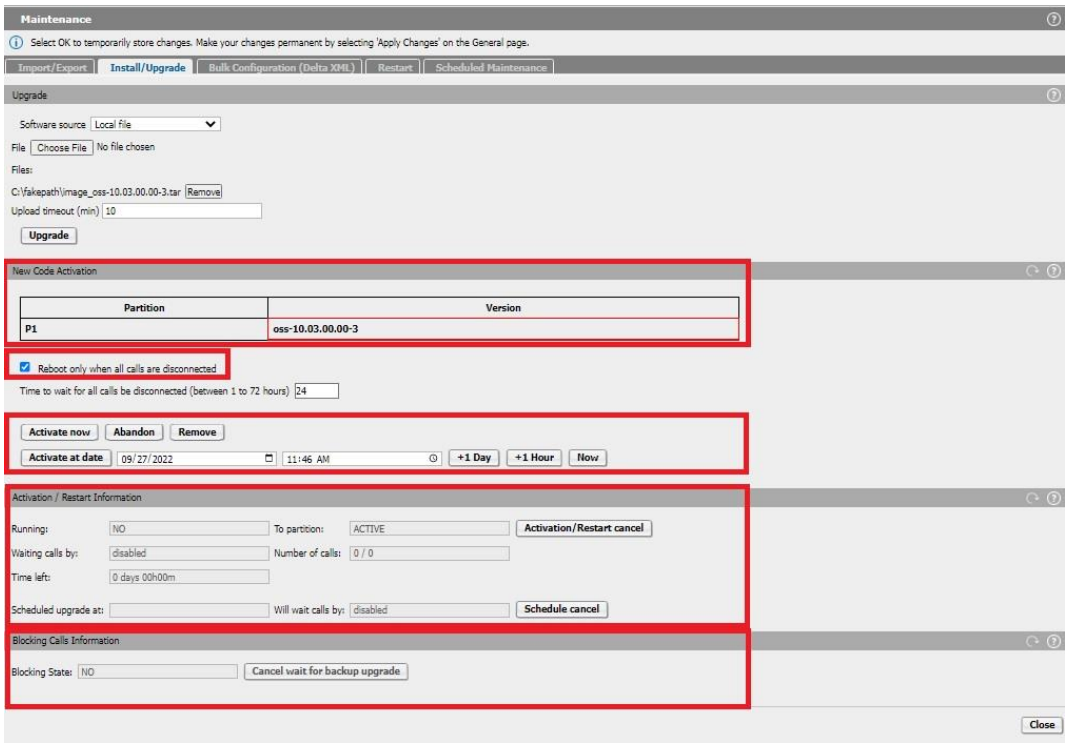
Another option is to back up the config file (before the upgrade) and if needed a full install can be done with existing DB for previous versions.

Upon the completion of the fallback, the browser's cache must be cleared prior to logging into the web admin interface.

4.2.2. Changes due to downtime reduction feature

Due to downtime reduction feature, the upgrade process was divided in two distinct procedures. The code partition upgrade is the first step. As done before, you will select the source code and upload it to the server.

After that, a new session in the GUI will be filled with the information about the new software. See below:



To proceed a normal upgrade as before, just press the button „Activate Now“and reboot to the new version.

When the “Abandon” button is used, an installed new partition will be ignored but left in the disk to be used if necessary. If a restart to it is done in the future, it will not upgrade a redundant node if the system is configured as a redundant pair.

When the “Remove” button is used, an installed new partition is set as empty, and it cannot be used later.

If you want to schedule the reboot time, then use the new option „Activate by date” to select the date when the activation of the new code will be done. See the full documentation about these new parameters.

The flag Reboot only when all calls are disconnected was added. If this flag is set, the upgrade is started only all calls are disconnected.

It is also possible to determine the time to wait for all calls be disconnected. The option is from 1 to 72 hours and the default value is 24 hours.

It is possible to cancel the Activation/Schedule to upgrade using the buttons in Activation/Restart Information.

NOTE1: The restart TAB also has changed, but the old buttons are still there. Read the full documentation if you are not comfortable with the new options.

NOTE2: For redundant system, when the flag "Reboot only when all calls are disconnected" is selected and upgrade is activated, the calls will be blocked until the end of upgrade process in both nodes (master and backup).

Activating the upgrade, the warning message must be shown indication it.

During this period, for instance, it is not possible to receive or generate calls and register subscribers.

However, it is possible to unlock the calls when the master node has already performed the upgrade and the backup node is not finished yet. For this, it is necessary to use the "Cancel wait for backup upgrade" button.

The "Cancel wait for backup upgrade" button is only available when calls are being blocked on the system by "pmc block" command.

4.3. Special settings and instructions

4.3.1. Redundancy

During initial installation, redundancy configuration must be done to each OpenScape SBC individually using its own physical IP Address. For redundancy configuration details, please see OpenScape SBC Configuration Guide.

4.3.2. Lenovo SR250/SR250 V2/V3, Lenovo SR530 and Lenovo SR630 V2/V3

When creating the USB stick for installation on Lenovo SR250/SR250 V2/V3, Lenovo SR530 or Lenovo SR630 V2/V3 platforms, the checkbox “Partitioned USB Stick” must be set.

To allow the booting from an USB drive, the following steps must be executed:

Power on or reboot the server.

When prompted, select F12 to enter Setup.

In “Boot Device Manager” selects “USB Storage” option.

Press Enter to exit.

IMPORTANT:

LEGACY MODE: Select F1 to enter in System Setup, choose UEFI Setup option, selects System Settings, the Legacy BIOS must be Enable. And the Boot Manager/Boot Modes must be configured as Legacy Mode.

UEFI MODE: Select F1 to enter in System Setup, choose UEFI Setup option, the Boot Manager/Boot Mode must be changed to UEFI mode. In System Settings, the Legacy Bios must be Disable.

4.3.3. OS-SBC Virtualization on VMWare

To install VM OS-SBC, please refer to the OpenScape SBC Configuration Guide, section 2.1.6.

When deploying vApps these values are set automatically (based on the 2.5 GHz core processor).

In OVF file in vApps, the CPU reservation is configured for Virtual OSS 250(5000 MHz), Virtual OSS 6000(10000 MHz) and Virtual OSS 20000(20000 MHz).

Regardless if VM was created manually or with vApps these values must be adjusted to fit the host processor capabilities and also considering other critical applications running at same host.

The recommended setting for the reservation is the number of cores used by OSB/SBC multiplied by the core frequency of host processor.

If the resources are not available in used VMWare Host server or due to the processor type, the following messages can be received in virtual machine power on:

“Failed - The amount of CPU resource available in the parent resource pool is insufficient for the operation. “

“Failed - Module 'MonitorLoop' power on failed.”

In this case, it is necessary to set the parameter Reservation to a value that fits in the host processor capabilities (considering also other applications) and parameter Limit=Unlimited.

In this case to avoid this risk is recommended to close monitoring the CPU usage at SBC. Alarms will be raised when the CPU usage is running high.

4.3.4. Licensing

OpenScape SBC will accept the CMP centralized licenses of the higher major version to allow smooth migration of customer environments during upgrade transition phases.

Standalone licensing for OpenScape Branch/SBC: For hardware machine, the license file must be generated with the eth0-MAC address of OpenScape Branch/SBC.

The license file should have a name as “<name>.lic”, for example, ALI_OpenScape_XXX_V10.lic or OSBV10_000245E1FACC.lic, when placed on the OpenScape Branch/SBC appliance.

The name of license file can be modified, but the file extension should remain as “.lic”. Do not use special characters on license file name.

Applying a standalone license file to an OpenScape Branch/SBC is done via the local GUI of OpenScape Branch/SBC -> System -> Licenses -> License Information Choose File and Upload the file.

Applying a license file/or allocating licenses to OpenScape Branch/SBC will result in a SIP Server restart and potential loss of existing calls.

Standalone licensing for virtual machines uses an Advanced Locking ID (ALI).

Be sure to configure OpenScape Branch/SBC to use the default gateway and be sure to have at least one DNS server in the DNS Server list (or check/enable the DNS Server box and provide the eth0 interface IP address as the DNS server address for purposes of calculating an ALI.

Then, this can be disabled after applying the license file).

An ALI can´t be requested if no DNS Server is configured.

The license file should be requested by providing the following information from virtual machine to generate an Advanced Locking ID (ALI). There is a folder Calculate Locking ID in CLS. **For a redundant OpenSCape Branch/SBC system, this information should be taken from the master node:**

Hostname of the OpenScape Branch/SBC: from Local GUI, System Info section -> Settings -> Hostname field.

Primary DNS Server: from Local GUI, navigates to Network/Net Services page -> DNS -> Client section -> DNS server IP Address list box and select the Primary DNS.

Default Gateway Address: from Local GUI, navigates to Network/Net Services page -> Settings -> Routing section -> Default Gateway Address field.

Host IP Address: from Local GUI, navigates to Network/Net Services page -> Interface Configuration section -> Access Realm Configuration box IP Address field of the Main IPv4 row.

Timezone: from Local GUI, navigates to Network/Net Services page -> NTP -> Timezone field.

NOTE: IF ANY OF THESE PARAMETERS WERE CHANGED, A NEW LICENSE FILE WILL BE REQUIRED.

There is another option to find the Advanced Locking ID. Goes to System -> License -> General -> Press Refresh button related to Advanced Locking ID. In this case, before to do it, configure the DNS Server and NTP Server.

The Advance Locking ID method in the previous bullet item is the recommended method to request a standalone license file for a OpenScape Branch/SBC in virtual machines.

This data is used to generate an Advanced Locking ID (ALI) and the license file will be generated with that ALI.

Applying a standalone license file to an OpenScape Branch/SBC is done via the local GUI of OpenScape Branch/SBC -> System -> Licenses -> License Information -> Choose File and Upload the file.

Applying a license file/or allocating licenses to OpenScape Branch/SBC will result in a SIP Server restart and potential loss of existing calls.

Floating licensing: The license file is locked with the MAC address or Locking ID of the Application Server (Common Management Portal)

After requested the license file, goes to CMP -> Maintenance -> Licenses -> Information -> Offline Activation -> Upload the license file and activate it.

To configure/allocate the licenses for OpenScape Branch/SBC, CMP -> Configuration -> OpenScape Branch or SBC -> select the OpenScape Branch or SBC -> Manage -> Configure the licenses.

Applying a license file/or allocating licenses to OpenScape Branch/SBC will result in a SIP Server restart and potential loss of existing calls.

IMPORTANT: Before to apply the license, please select the OSB or SBC and press "Refresh Selected" button to update the used "Version" field in CMP side. Then, apply the desired license.

NOTE1: If the customer has the invalid license due to hardware or configuration changes, the OpenScape Branch/SBC will go to into the grace period of 30 days to allow the fix of license problem.

NOTE2: For a redundant OpenScape Branch/SBC system, apply the license file only on the master node by logging into Local GUI via the VRRP address to the OpenScape Branch/SBC system.

NOTE3: Some licenses are not applied via CMP for OpenScape SBC system. For instance, SBC_OSEE_interworking license.

4.3.5. OS-SBC Configuration Related Recommendations

The following Private IPs should be added to the firewall blacklist since they can be used as spoofed address on a DOS attack.

0.0.0.0/8

14.0.0.0/8

24.0.0.0/8

172.16.0.0/12

169.254.0.0/16

127.0.0.0/8

If a VLAN is enabled and using an IP address from one of the above subnets, then a blacklist firewall rule for that particular VLAN Network ID must not include this VLAN subnet.

4.3.6. SIP Trunk (SSP) Certification

SIP Trunk testing is required to ensure reliable interoperability and on going support from Global Service, and also the SIP service provider (SSP), it the SSP operates a mandatory certification program.

SIP Trunk testing is required the first time the OpenScape Voice Solution (OpenScape Voice, OpenScape SBC, Oracle (Acme Packet) SBC and/or OpenScape Branch) is connected to a SSP or if the SSP changes their interface since the original test.

The lists of the Providers, which have been tested and released with the enterprise platform is located here.

Since the SIP Trunk interfaces on the OpenScape Enterprise solution are backwards compatible, retesting is not mandatory for each new version of the solution unless mandated by the SSP; however, it is strongly recommended.

4.3.7. OpenScape Branch/SBC Single load line concept

With the implementation of the Single Load line feature, the handling of bug fixes, security updates and even fast features is improved.

The features from OpenScape Branch/SBC V9R4 onwards received an internal flag and based on the actual version of the OSB/SBC License file, the feature will be enabled or not of new features.

For example, V9 features require a V9 or higher OSB/SBC License file to be enabled.

It is also planned to all the functionality of some smaller enhancement that would not require a license file check, therefore becoming available independently of the OSB / OS-SBC License file.

The CMP or Local GUI can display the version of the OSB/SBC Base License file. See the applied license under Administration -> System -> License -> License Information.

The Base License Version and the SIEL ID will be stored in XML file.

If no License Version is available or no License is applied (Grace period) the OSB / OS-SBC will enable the Implementation/Feature set based on current version.

4.3.8. OS-SBC Maintenance Mode

- Maintenance mode in OS-SBC is a way to set the SBC call processing in an out of service state, so the traffic can be handled by another server, without shutting down the server. In that way, the upgrade and configuration functionalities can still be done.
- In case of scheduled Maintenance administrators are responsible to redirect traffic to another SBC (in case the topology of the network does not support rerouting automatically) during maintenance window. After this new implementation there is the possibility of scheduling automatically the maintenance mode only when there are no active calls in the system.
- Additionally, in case of scheduled Maintenance mode if flag “In Maintenance only after calls are disconnected” is set, active calls are not affected at any way before “Time to wait for all calls be disconnected (between 1 to 72 hours)” is reached. Although, all new calls will be rejected, until Maintenance mode is activated. Statistics will be working in maintenance mode and ongoing calls can still be monitored in the Management Portal in Diagnostics & Logs menu and in Statistics Tab.

4.3.9. SBC Upgrade to V11R3 from V10R3 with Circuit Remote Endpoint

Before any upgrade from V10R3, the Remote Endpoints related to Circuit must be removed/changed since SBC V11 does not support Circuit functionality.

Please pay attention for any "hidden" (Circuit) Remote Endpoint (in case of disabled “Enable Remote Endpoints”).

5. Hardware and Software Compatibility

5.1. Hardware

Hardware model	Revision	End of Support Date (M44)
Fujitsu Primergy RX200 S6 Dual 6C Intel X5650 2.7GHz	BIOS V6.00 R1.10.3031	October 7th, 2019
Fujitsu Primergy RX200 S7 Dual 6C®te®) Xeon(R) CPU E5-2620 0 @ 2.00GHz	BIOS V4.6.5.3 R2.4.0	December 5th, 2022
IBM x3250 M3 4C Intel X3430 2.4GHz	BIOS V 1.07	August 4th, 2020
IBM x3550 M3 Dual 6C Intel X5650 2.67GHz	BIOS V 1.08	April 7th, 2020
IBM x3550 M4 Dual 6C®te®ntel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	BIOS D7E124AUS-1.30	April 15th, 2022
IBM x3250 M5	BIOS V1.00	December 31st, 2023
LENOVO x3250 M6	BIOS V2.0	June 30th, 2025
LENOVO x3550 M5	BIOS V1.11	March 30th, 2025
LENOVO SR530	UEFI Version 3.00 TEE172F	November 1st , 2029
LENOVO SR250	UEFI Version 2.50 ISE124C	November 1st , 2029
LENOVO SR250 V2	UEFI Version 1.20 TQE108D	November 1st , 2034
LENOVO SR630 V2	UEFI Version 1.51 AFE122I	November 1st , 2034
LENOVO SR250 V3	UEFI Version 8.10 CTE122E	*
LENOVO SR630 V3	UEFI Version 3.60 ESE134E	*

NOTE: All End of Support (M44) dates not marked in red indicate active support periods. You can verify this by comparing the listed date in the table to the current date.

NOTE: For questions about the End of Support Date (M44), refer to the End of Sales Circulars or the document Unify OpenScape Branch 1000 V11 - Guideline OpenScape Branch Hardware Status Relative to V11. Download the guideline document Here

NOTE: For hardware/server security and safety advisories, please refer to the manufacturer's websites.

NOTE: For Lenovo SR530, SR250, SR250 V2, SR250 V3, SR630 V2 and SR630 V3 the mentioned BIOS were used to UEFI Mode tests.

5.2. Firmware

5.2.1. Unify policy for Lenovo firmware updates

Unify policy allows but does not require Lenovo firmware updates with versions greater than the version listed in OSV, SBC or Branch Release Notes.

1. Unify will support OpenScape homologated servers running the firmware version equal to or greater than the firmware version listed in the OSV, SBC, and Branch Release Notes (typically the version at homologation). This covers the case of Lenovo delivering servers with updated firmware, as well as customer updating the firmware for their own reasons (i.e. to fix security vulnerability, etc...)

2. Unify does not require that the server firmware be updated (unless the firmware version is older than the version listed in the Release Notes).
3. Instances of OSV, SBC or Branch software that have suspected failures related to a supported firmware version should have a ticket raised so that issues with firmware versions can be confirmed and documented in OSV, SBC and Brach Release Notes.
4. Servers are homologated based on Lenovo System (x3550 M5), Type (8869), Model (AC1) and Ordered Product Model (U09FLA1). These values should be verified using the physical servers Serial Number, using Lenovo's support Website before server hardware is assumed to be changed from original homologation.
   NOTE: The Service detected during the limited period, the faulty firmware installation from LENOVO in x3550 M5 hardware. In this case, it is recommended to update the firmware.

Lenovo Online SAS/SATA	L365
Lenovo System x2550 M5 UEFI	2.81
Intel v23.2 Network	1.1937.0
Broadcom NX-1 Ethernet	212.0.5.4
BIOS	24.21.0-0064
Integrated Mgmt Module	5.11

5.3. Loadware

Not applicable for this product

5.4. Software / Applications

This release note contains information pertinent to the OpenScape SBC software only. Additional software products are required to install and operate the OpenScape SBC.

These products are listed in the following table, including their respective versions required to use with the current OpenScape SBC software.

Product	Software Version	Status	Nuxeo-KMOSS Note
OpenScape Voice Assistant ***For OSV V9***	9.0_0.15.0-124 (V9R0.0.x)	GA	-
OpenScape Voice Assistant ***For OSV V10***	9.3_0.109.0-436 (V10R0.4.x)	GA	-
OpenScape Branch Assistant ***For OSV V9***	8.0_0.36.0-174 (V9R0.0.x)	GA	-
OpenScape Branch Assistant ***For OSV V10***	8.0_0.66.0-275 (V10R0.4.x)	GA	-

TLS versions supported: V1.0, V1.1, V1.2 and V1.3

5.5. Operating systems

Operating System Name	Operating System Version
Linux	**Based on OpenScape Branch Linux Distribution Leap 16.0**

5.6. Compliant products

This section lists the versions associated with the communication platforms, other products and third-party products that have been tested for use with this version of the product and are known to work.

5.6.1. Communication platforms

Hardware and software products that have been tested together with this version of the product are listed in the common compatibility matrix, which also includes the respective versions required to use with the current version of this product.

The current Common Compatibility Matrix can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

Note: Use the "Search & Find" option under Portfolio Information and Search Documentation for "Common Compatibility Matrix" (search on title only!).

The current Common Compatibility Matrix can also be found on the Nuxeo:

https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/19807d7c-2588-4c6c-ad1b-5f20d509191d

5.6.2. Other products

- Image to OpenScape 4000 hosted SBC (bz2 file):

This image is available to OS4K (hosted SBC) and the use is tested successfully and released by the OS4K Group.

Deployments on an OS4K (hosted SBC) requires a minimum OS4K Platform version of V8R2.22.6 or V10R0.28.1.

From OS4K Platform version V10R1.28.0, please use the OpenScape SBC V10R2.3.0 version or higher.

Note1: Now, it is possible to change the branding Product Name in OpenScape SBC, but after upgrading it returns to default Branding Name.

Note2: The correction related to OSFOURK-24929 is available from V10R1.42.1 PLT.

Note3: Before upgrading OS4K version changing the Release (for example: OS4K Platform version from V10R0 to V10R1), it is recommended to back up the openScape SBC database.

5.6.3. Third-Party products

Not applicable for this product.

6. Service Information

6.1. Management information base

☒ Product sends SNMP V2 traps ☒ Product sends SNMP V3 traps ☐ Not supported

6.2. License management

This product is licensed using:

☒ CLS ☐ CSC ☐ Other or not relevant, as described below.

6.3. Remote serviceability

This product is certified for the following:

☐ RSP ☐ HiSPA ☐ RTPatch ☒ Other remote access or not relevant, as described below.

Type of Installation	Transfer time via SIRA/HiSPA/SSDP	Installation Time
Initial Installation	Approximately 3 minutes	Approximately 15 minutes
Delta Installation	Approximately 3 minutes	Approximately 10 minutes

Hints for remote serviceability: See OpenScape SBC Configuration Guide.

6.4. Product tooling structure

Release Notes for OpenScape SBC can be found in Nuxeo-KMOSS. Binary files are distributed via SES. The following table illustrates how to find the currently supported OpenScape SBC software in Nuxeo-KMOSS/SWS.

Main Category	Communication Systems
Product Family	OpenScape SBC
Product	OpenScape SBC
Product Version	OpenScape SBC V11
Product Item #	P30152-P1641-B1-20 (V11R3.4.0)

6.5. Case tracking system

Tickets can be generated and tracked via the WEB Support Portal (AWSP).

http://atosunify.service-now.com/unify

A short instruction can be found on the AWSP directly.

7. Documentation Reference

The product documentation can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

8. References

Further related information can be found under the following links:

HF006979