Release Notes

Release Notes Version: V1.10, 2024-07-15

Atos Unify OpenScape 4000 V11

Software Version: V11 R0.22.0

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

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

Deliverables

☒ Full Release ☐ Delta Release

Export Control Classification Data

AL: 5D002C1A ECCN: 5D002ENC3

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

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Table of Contents

1 History of Change

1.1 Release notes content

Version	Date	Description of changes
1.0	2023-11-29	Initial creation
1.1	2024-02-29	Update chapter 2, 3 & 4
1.2	2024-03-08	Update chapter 1.1, 3.1
1.3	2024-03-21	Update chapter 2.2, 3.1 & 4.1
1.4	2024-03-27	Update chapter 2.1.1, 3.1, 3.2 & 4.2
1.5	2024-04-03	Update chapter 2.1.1
1.6	2024-03-11	Update chapter 2.1.1.2 & 3.3
1.7	2024-04-22	Update chapter 3.1, 3.2 & 4
1.8	2024-06-19	Update chapter 2 & 3
1.9	2024-07-01	Update chapter 3 & 4
1.10	2024-07-15	Update chapter 3

1.2 Product versions history

Software Version	Production Version	Date	Remarks
V11 R0.22.0		2024-03-22	GA

2 Changes

2.1 Implemented Change Requests / New features

2.1.1 New in V11 R0

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-25976	Internal VPN V11R0 compatible with SG B0 on PLT V10R1.42	
	OSFOURK-25069	V11 Platform Portal clean-up	
	OSFOURK-24611	Improve RMX HF activation time	
	OSFOURK-24512	Introduce V11 licensing	
	OSFOURK-23695	Migrate from SLES15 to OpenSuse Leap 15.5	
	OSFOURK-23598	Centralized IP address for SoftGate - HFA	
	OSFOURK-23363	UI Control board for container framework.	

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-23362	Introduce Kubernetes/Docker framework to OS4k platform SW	
	OSFOURK-23347	Show PSU Status of Eco/Branch in Sysinfo	
	OSFOURK-23223	Improve manual consultation from Agent with STAOND	
	OSFOURK-23195	Configuration of an email address for 4K station in RMX via AMO PERSI	
	OSFOURK-23165	CMI: Make call log handling on mobile devices more user friendly and performant	
	OSFOURK-23164	CMI: Make phone book search on mobile devices more user friendly and performant	
	OSFOURK-23059	OND caller ID handling	
	OSFOURK-23057	Info field in AMO CGWB for Gateway Manager and HG WBM	
	OSFOURK-23055	TLS 1.3 on VoIP interfaces	
	OSFOURK-23054	Software Subscription Licensing V3 for OpenScape 4000	
	OSFOURK-22996	Increase number of WABE/VBZ/VFGR from 16 to 64 in RMX	
	OSFOURK-22995	Introduce new language Czech with diacritic characters in OS4K	
	OSFOURK-22994	Playing an announcement for special call forwarding scenarios	
	OSFOURK-22993	A-law µ-law conversion configurable per DIUT3 in the same system	
	OSFOURK-22988	Assistant dashboard: should show running applications (like iSBC) together with resp. HW	
	OSFOURK-22971	OS4k hunt group support by Unify Phone	
	OSFOURK-22967	Online connection to CLS for OS4k and OS4k Manager via Cloud CLA	
	OSFOURK-22964	Hunt group: outgoing calls with "Hunt Group" master phone number	
	OSFOURK-22963	CMI: Call Journal improvement for cordless devices after consultation calls	
	OSFOURK-22900	ADD-ACMSM change APPLNO automatically if position is busy	
	OSFOURK-22768	Improve the message in UC call control when calling party has PD busy	
	OSFOURK-22740	M5T Stack update vHG	

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-22680	Report Agent ready event after agent logged on event in case of autologon	
	OSFOURK-22495	CHANGE-WABE entries are not displayed when using REG-WABE:DPLN=0&&15,TYPE=GEN;	
	OSFOURK-21872	Support of Traditional Chinese	
	OSFOURK-21840	Move SBCSU device type (example: "*) DPCP") in "Inherited attributes" field	
	OSFOURK-21383	UC- SST response to master HG contains GRP number in Control Redirection Party	
	OSFOURK-20374	CSTA and UC integration for DNIT and SA nodes	
	OSFOURK-20245	Do not allow overwriting of a protocol before deactivation	
	OSFOURK-19712	Group names are not delivered in the CSTA interface for Group members -> ACL origDialedNumber as party	
	OSFOURK-19309	WebRTC video REFER is passed to client instead of being processed by vHG	
	OSFOURK-18683	Display logged in AGENTS (AMO AGENT)	
	OSFOURK-18642	CEXTPD: new configurable timer	
	OSFOURK-18446	STMIY, successor of STMIX	
	OSFOURK-18428	Common License Handling for OS4K and affiliate applications ("User oriented licensing")	
	OSFOURK-16974	Improve OLED FI to allow primary or secondary choice	
	OSFOURK-16853	Allow SPE for Native SIP Trunk without SIPCO/ZANDE checks	
	OSFOURK-14263	Do not allow KNDEF with single node level configuration if ZAND PNNO is already multi-level	
	OSFOURK-10323	UFIP MASK in SBCSU	
	OSFOURK-9443	System Reload after Auto-GENDB	
	OSFOURK-9221	OS update optimization	
	OSFOURK-7395	Apply Assistant/Manager Login banner also to Platform and CSTA SSH	
	OSFOURK-7101	Allow remote Factory Reset possibility for STMIX and STMIY	
	OSFOURK-6781	Platform Portal: offer configuration of SG WAN interface (bonded/unbonded) in LAN wizard for SoftGate	
	OSFOURK-6671	Include preparation step that REGEN/GENDB is being called.	
	OSFOURK-4713	Portal - installation status: display hint when DELTAs occurred after FI Auto-GENDB	

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-4645	OS-Update install kit for SG, STMIX, EcoAP shall use the SG package from LW Hotfix, not the one from Platform image	
	OSFOURK-3329	Change of default GW UIMODE : MAINTAIN	
	OSFOURK-2387	Centralizing and forwarding of alarm and error logs of OS4K LINUX SW Appliances via syslog mechanism.	

2.1.1.1 Assistant / Manager

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-24512	Introduce V11 licensing	
	OSFOURK-24275	Manager: provide Secure Mode for Platform	
	OSFOURK-24273	central core file handling for /var/crash core files	
	OSFOURK-23389	Allow access of existing PLT, CSTA and Assistant trace interfaces from Perm Trace	
	OSFOURK-23171	Integration of RSP Servicelink	
	OSFOURK-23158	Generate a graphical 4K system diagram from the configured system	
	OSFOURK-23156	Set Assistant engr password globally for all appliances having an Assistant	
	OSFOURK-23106	Display license information for EntGW/SoftGate	
	OSFOURK-23058	Automatic platform HF activation for OS4k system (host plus all APs)	
	OSFOURK-23057	Info field in AMO CGWB for Gateway Manager and HG WBM	
	OSFOURK-23056	Central license upload for EntGW/SoftGate	
	OSFOURK-23054	Software Subscription Licensing V3 for OpenScape 4000	
	OSFOURK-22988	Assistant dashboard: should show running applications (like iSBC) together with resp. HW	
	OSFOURK-22967	Online connection to CLS for OS4k via Cloud CLA	
	OSFOURK-20374	CSTA and UC integration for DNIT and SA nodes	
	OSFOURK-20055	Enhance Assistant interface for CMP to create Unify Phone clients	
	OSFOURK-18428	Common License Handling for OS4K and affiliate applications ("User oriented licensing")	
	OSFOURK-17960	Default MAINTAIN UI mode for GWs	
	OSFOURK-17825	Perm. Logging: centralize trace and log interfaces (Ass, CSTA, PLT)	
	OSFOURK-17610	SWM SWS extend UI customer, type, country and EULA selection	
	OSFOURK-16212	CM: do not store data older than 90 days in uc_action_log table	
	OSFOURK-16201	Improve Assistant reinstallation mechanism	
	OSFOURK-14746	DLS error codes when synch with Manager should be improved with the corresponding - text	

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-14405	Local restore of restore settings, regardless that external HBR is used	
	OSFOURK-12180	Automated Phone SW handling in IPSM	
	OSFOURK-9273	Auto configure AP Backup server to all Surv Units	
	OSFOURK-7395	Apply Assistant/Manager Login banner also to Platform and CSTA SSH	
	OSFOURK-6671	Include preparation step that REGEN/GENDB is being called.	
	OSFOURK-4600	Assistant dashboard: display hint when STMIX/SoftGate/EntGW have inconsistent SW	
	OSFOURK-2387	Centralizing and forwarding of alarm and error logs of OS4K LINUX SW Appliances via syslog mechanism.	
	OSFOURK-24512	Introduce V11 licensing	
	OSFOURK-24275	Manager: provide Secure Mode for Platform	
	OSFOURK-24273	central core file handling for /var/crash core files	
	OSFOURK-23389	Allow access of existing PLT, CSTA and Assistant trace interfaces from Perm Trace	
	OSFOURK-23171	Integration of RSP Servicelink	
	OSFOURK-23158	Generate a graphical 4K system diagram from the configured system	
	OSFOURK-23156	Set Assistant engr password globally for all appliances having an Assistant	
	OSFOURK-23106	Display license information for EntGW/SoftGate	
	OSFOURK-23058	Automatic platform HF activation for OS4k system (host plus all APs)	
	OSFOURK-23057	Info field in AMO CGWB for Gateway Manager and HG WBM	
	OSFOURK-23056	Central license upload for EntGW/SoftGate	
	OSFOURK-23054	Software Subscription Licensing V3 for OpenScape 4000	
	OSFOURK-22988	Assistant dashboard: should show running applications (like iSBC) together with resp. HW	
	OSFOURK-22967	Online connection to CLS for OS4k and OS4k Manager via Cloud CLA	
	OSFOURK-20374	CSTA and UC integration for DNIT and SA nodes	
	OSFOURK-18428	Common License Handling for OS4K and affiliate applications ("User oriented licensing")	
	OSFOURK-17960	Default MAINTAIN UI mode for GWs	
	OSFOURK-17825	Perm. Logging: centralize trace and log interfaces (Ass, CSTA, PLT)	
	OSFOURK-17610	SWM SWS extend UI customer, type, country and EULA selection	
	OSFOURK-16212	CM: do not store data older than 90 days in uc_action_log table	
	OSFOURK-16201	Improve Assistant reinstallation mechanism	
	OSFOURK-14746	DLS error codes when synch with Manager should be improved with the corresponding - text	

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-14405	Local restore of restore settings, regardless that external HBR is used	
	OSFOURK-12180	Automated Phone SW handling in IPSM	
	OSFOURK-12179	Automated Phone SW handling in TSDM / IPSM	
	OSFOURK-9273	Auto configure AP Backup server to all Surv Units	
	OSFOURK-7395	Apply Assistant/Manager Login banner also to Platform and CSTA SSH	
	OSFOURK-6671	Include preparation step that REGEN/GENDB is being called.	
	OSFOURK-4600	Assistant dashboard: display hint when STMIX/SoftGate/EntGW have inconsistent SW	
	OSFOURK-2387	Centralizing and forwarding of alarm and error logs of OS4K LINUX SW Appliances via syslog mechanism.	
	OSFOURK-12942	MGR the Level 2 (Ebene 2) radio button should be disabled/greyed out for any other key than NAME	
	OSFOURK-22614	support of ECDSA ciphers and certificate for SIP (SG/STMIX)	
	OSFOURK-23361	Ability to define more than one dedicated eth port for SIP Client interfaces	

2.1.1.2 Decoupled Features in V11 R0

Tracking Reference	Internal Reference	Summary	Released in Version
	OSFOURK-25646	Adapt OS4K Assistant DLS API calls to new OSEM API	
	OSFOURK-23374	RFC 5139 support - Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)	
	OSFOURK-23350	Allow easier roll back and roll forward during RLC upgrades	
	OSFOURK-22494	DIS-VADSU memory usage optimization	
	OSFOURK-17694	Support of private number / authentication number in PAI on native SIP trunk	
	OSFOURK-2541	Customers wish to be able to reset appliance components to factory default	
	OSFOURK-24898	Integration of Remote Service Plugin (RSP) Servicelink - Self Registration for OpenScape 4000 in SIRA	
	OSFOURK-20055	Enhance Assistant interface for CMP to create Unify Phone clients	
	OSFOURK-26572	Installation of Kubernetes Layer and OSEM on standard EcoServer SSD (240GB) inclusive RAID support	Platform Hotfix V11 R0.22.1

2.2 Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary	Released in Version
	DWE-19729 DWEH-5771	WSI feature does not work, update to CP HFA 1.7.5.0054	V11R0.22
	OSFOURK-26360	Manager: CM uxsdbsyn daemon restarts and upload all for VNR is still running	V11R0.22
	OSFOURK-26376	RLC16_OSCC agent unable to make call to DNIT	V11R0.22
PRB000072782	OSFOURK-26443	E.164 numbers incorrectly handled in ACL when overlapping is used	V11R0.22
PRB000072793	OSFOURK-26442	Assistant LogMEvtLog daemon crash	V11R0.22
PRB000072606	OSFOURK-26213	For outgoing call from hunt group member wrong characters can be seen at called network party	V11R0.22
	OSFOURK-26288	In case UC cust with Hunt Group, ACL Offered event and ACL ring event for HG members are not translated to CSTA	V11R0.22
	OSFOURK-26272	move of UFIP station fail - device combination cannot be installed at a bus	V11R0.22
PRB000072706	CMI-568	DTB- "Faster access to DTB menu, the "long press" also works if no DTB is configured, and the phone then switches to dial mode	V11R0.22
PRB000073694	OSFOURK-26560	BLF client with SSL is not connected	V11R0.22
PRB000073350	OSFOURK-26565	Payload on stations from first shelf of Extended Enterprise Gateway is lost after CC restart	V11R0.22
PRB000073518	OSFOURK-26117	Unify Phone E-Mail Addresses gone after updating from V10 R1 to V11 R0	V11R0.22
PRB000071774	OSFOURK-26060	CM - UFIP station cannot be administrated in Manager	V11R0.22
PRB000072959	OSFOURK-26490	GWM License Upload failed with Firefox	Use another browser
PRB000072609	OSFOURK-26446	KNMAT/REPEXT incorrectly used in case of outgoing external call from hunt group member	V11R0.22

2.3 Resolved Vulnerabilities

Tracking Reference	Internal Reference	Summary	Released in Version	Severity Level
	OSFOURK-26299	PSA V11R0: Arbitrary File Upload in HBR	V11 R0.22.0	Medium
	OSFOURK-26071	PSA V11R0: unauthenticated Command Injection vulnerability affecting Emergency Password Reset feature	V11 R0.22.0	Critical

Tracking Reference	Internal Reference	Summary	Released in Version	Severity Level
	OSFOURK-26199	PSA V11R0: SQL Injection vulnerability in checkPassword.cgi.en_US	V11 R0.22.0	Medium
	OSFOURK-26200	PSA V11R0: SQL Injection vulnerability in setAlarmConfiguration.cgi.en_US	V11 R0.22.0	Medium
	OSFOURK-26233	PSA V11R0: authenticated Command Injection in prpr_api.cgi	V11 R0.22.0	Medium
	OSFOURK-26206	PSA V11R0: SQL Injection vulnerability in showSNMPData.cgi	V11 R0.22.0	Medium
	OSFOURK-26245	PSA V11R0: authenticated command injection vulnerability in wsm.cgi	V11 R0.22.0	Medium
	OSFOURK-26238	PSA V11R0: authenticated Command Injection in secmode/index.cgi	V11 R0.22.0	Medium
	OSFOURK-26297	PSA V11R0: Business Logic vulnerability giving rsta and rsca users root permission	V11 R0.22.0	Low
	OSFOURK-26230	PSA V11R0: authenticated Command Injection in snmpControl.cgi.en_US	V11 R0.22.0	Medium
	OSFOURK-26300	PSA V11R0: Reflected XSS in rds_gui.cgi	V11 R0.22.0	Low
	OSFOURK-26244	PSA V11R0: authenticated command injection vulnerability in api_ngtc.cgi	V11 R0.22.0	Medium

Tracking Reference	Internal Reference	Summary	Released in Version	Severity Level
	OSFOURK-26318	PSA V11R0: Reflected XSS in in content2.pl	V11 R0.22.0	Low
	OSFOURK-26319	PSA V11R0: Reflected XSS in index.pl	V11 R0.22.0	Low
	OSFOURK-26317	PSA V11R0: Reflected XSS in backServ.pl	V11 R0.22.0	Low
	OSFOURK-26325	PSA V11R0: Reflected DOM XSS in backServ.pl	V11 R0.22.0	Low
	OSFOURK-26333	PSA V11R0: Host Header Poisoning	V11 R0.22.0	Low
	OSFOURK-26243	PSA V11R0: authenticated Command Injection in webmin save_tz.cgi	V11 R0.22.0	Medium
	OSFOURK-26248	PSA V11R0: authenticated Command Injection sws.cgi	V11 R0.22.0	Medium
	OSFOURK-26232	PSA V11R0: authenticated Command Injection sws.cgi	V11 R0.22.0	Medium
	OSFOURK-26323	PSA V11R0: Stored XSS in getSecMUserData.cgi	V11 R0.22.0	Low
	OSFOURK-26231	PSA V11R0: authenticated Command Injection sws.cgi	V11 R0.22.0	Medium

Tracking Reference	Internal Reference	Summary	Released in Version	Severity Level
	OSFOURK-26237	PSA V11R0: authenticated Command Injection in secmode/index.cgi	V11 R0.22.0	Medium
	OSFOURK-26301	PSA V11R0: Reflected XSS in connect.pl	V11 R0.22.0	Low
	OSFOURK-26080	PSA V11R0: authenticated Command Injection in APPM api.cgi	V11 R0.22.0	Medium
	OSFOURK-26229	PSA V11R0: authenticated Command Injection in api911.cgi	V11 R0.22.0	Medium
	OSFOURK-26250	PSA V11R0: SQL Injection vulnerability in editUser.cgi.en_US	V11 R0.22.0	Medium
	OSFOURK-26226	PSA V11R0: Command Injection in Backup and Restore	V11 R0.22.0	Medium
	OSFOURK-26316	PSA V11R0: Reflected XSS in save_servAccess.cgi	V11 R0.22.0	Low
	OSFOURK-26302	PSA V11R0: Reflected XSS in save_host.cgi	V11 R0.22.0	Low
	OSFOURK-26321	PSA V11R0: Reflected XSS in save_tz.cgi	V11 R0.22.0	Low
PRB000076413	OSFOURK-27410	Command injection vulnerability in platform portal which may allow an unauthenticated attacker to execute OS commands as wwwrun	V11 R0.22.0	CVSS Base score: 9.8 (critical)

3 Important Issues, Workarounds, Hints and Restrictions

3.1 Important Issues

Tracking Reference	Internal Reference	Summary	Workaround / Actions
	OSFOURK-27051	Monitoring events not working in case of Attendant console answers the call	Fixed with RMX HF1
	OSFOURK-26941	Assistant - Col_schedule is directly dependent of pm_col daemon	Activate PM from Application Control before using Col
	OSFOURK-20011	Auto REGEN&GENDB might show a GENDB delta related to DIMSU/CCIDXD parameter	Fixed with PLT HF1, it needs to be transferred together with the RLC
	OSFOURK-27028	DTB server crash when a call from a DTB user to a non-DTB user is answered, requires manual intervention to restart DTB resource	Fixed with PLT HF1
	OSFOURK-24314	Other SDAT attributes will be lost during GENDB run if attribute STAOND is present in the same CHA-SDAT command	Fixed with PLT HF1, it needs to be transferred together with the RLC
	OSFOURK-26784	SPE SIPQ trunk not working with ECDSA certificate	Use RSA based certificates for boards having SIPQ trunk configured
	OSFOURK-26762	RISO & RecoveryHD does not support 4Kube & OSEM	Fixed with PLT HF1
	OSFOURK-26924	OSEM not accessible on Standalone EntGW	Fixed with PLT HF1
PRB000072461	OSFOURK-26394	Configuring on STMI board a Management IP with CGWB MANLANIF needs additional RES-BSSU	If these parameters are changed, the boards have to be reset twice in order to obtain the modified data. The first reset provides the new configuration data to the affected boards and the second reset activates it.
	OSFOURK-26884	Cloud CLA - Settings are lost after NUC from eFT version (V11R0.19)	Fixed with Assistant HF1
	OSFOURK-26909	RISO Restore does not work properly.	Remove EFI folder from USB Stick and ensure system boots from USB Stick by plugging out the SSDs and booting the USB Stick alone and insert back the SSDs only when the Stick asks for Recovery confirmation.
	OSFOURK-26886	CM Personal data - Subscriber config not saved	Fixed with Assistant HF1
	OSFOURK-20516	Assistant - IPDA Wizard not working when adding an Extended Enterprise Gateway	Make the changes via AMO commands

Tracking Reference	Internal Reference	Summary	Workaround / Actions
		RLC upgrade will fail if Auto REGEN&GENDB takes more than 3 hours to finish during the Activation	Repeat separately Auto REGEN&GENDB and choose the second option "Use current RMX DB for the RLC update and ignore SWU GENDB DELTAS if present"
	OSFOURK-23714	recovery-H4K on Simplex not working	Use portal LAN Wizard or first install
	OSFOURK-25849 OSFOURK-22373	Unable to upload a backup set from V10 or older	If issue is noticed, change owner for below folder chown root:unity /.AS/BACKUP/IO_BUF_TRANS/INPUT/
	OSFOURK-21273	RLC activation can fail if USB console cable plugged	takeout USB cable before activation
	OSFOURK-26133	System may remain in Y if OS4K ISO is removed before GENDB is finished	do not remove ISO during GenDB
	OSFOURK-26939	Unable to synchronize OSFM with OS4K V11 R0.22.0	Under investigation
	OSFOURK-17798	If both OSMO and WebRTC are involved in consultation/large conference/CFNR scenarios, OSMO calls are dropping when SMP=YES	
	CMS-6352	No video views in both directions during MS conference when OSMO users are involved	
	OSFOURK-17766	Payload missing on OSMO after Hold/Retrieve from UC when SMP=YES	
PRB000064994	OSFOURK-24213	Improve RISO behaviour in case RISO creation fails (e.g. no connection to SFTP server), as the process remains stuck and can't be cancelled /restarted	The riso controller may be restarted from the platform of the affected node `crm resource restart rsc4k_risocontroller`
PRB000065627	OSFOURK-24130	RISO GUI page (Appliance Management) does not show all Backups	
INC003305655	OSFOURK-22963	CMI: Call Journal improvement for cordless devices after consultation calls	
		HFA phones - TLS 1.3 for HFA not working reliably for HFA phones on SG and STMIX	Will be fixed with LW HF1 for V11R0.22 and HFA next phone SW release
	OSFOURK-27108	CC restart after PROC INT@UA:1C88:0DEC when running DIS-KNDEF or REG-KNDEF with NODEINFO longer than 22 characters	Fixed with RMX-HF1

Tracking Reference	Internal Reference	Summary	Workaround / Actions
	OSFOURK-27622	SoftGate on VMware 4GB RAM with OSEM enabled restarts during RISO backup	add 2 additional GByte RAM
PRB000077769	OSFOURK-27727	Rufus tool (Version 4.2 or higher) prints a warning message "Zurückgezogenes UEFI Startprogramm erkannt" / "Revoked UEFI boot loader detected" when writing a bootable OS4K ISO image to an USB stick.	Ignore the warning. OS4K install images are safe and secure when downloaded directly from SWS

3.2 Workarounds, Hints

Tracking Reference	Internal Reference	Summary	Workaround / Actions
		No optional patches are available with V11R0.22.0	Patches will be provided upon customer request
	OSFOURK-26407	Auto REGEN&GENDB will finish with deltas if there are HOTLN entries configured with external destinations (TIE/CO)	Repeat separately Auto REGEN&GENDB and choose the second option "Use current RMX DB for the RLC update and ignore SWU GENDB DELTAS if present" and add the missing HOTLN commands after the upgrade to V10 R1.42
		After successful HW/SW installation, USB sticks should be removed from the EcoServer/EcoBranch to avoid unwanted boot behaviours.	Remove USB stick after installation
		BIOS settings of OpenScape 4000 EcoServer/EcoBranch HW should not be modified.	
		An IP security scan can have significant impact on OpenScape 4000 real time communication system components. It is recommended only to perform security scans outside of core business hours as internal health checks can be interrupted, which may result in a restart due to the system's automated recovery processes. HINT: Additionally, as per the OpenScape 4000 Security Checklist, "Secure Mode" can be activated for some components to limit the number open IP ports.	
		The preferred method for configuring SIP Subscribers is UFIP. Solutions will	

Tracking Reference	Internal Reference	Summary	Workaround / Actions
		only be delivered based on UFIP configuration. Should any UFIP feature discrepancy be noticed to the prior S0PP configuration then it should be reported via customer ticket. Longer term S0PP will be removed.	
		Installations should only be made using XML files (no other method is supported). ComWin version 5.0.149 (or higher) from SWS is recommended which includes the XML Config File Generator.	
		For classic cleartext FAMOS connection, which do not yet support the secure option enable the FAMOS port 102 in Assistant firewall settings	
	OSFOURK-20479	NUC from V10 + PLT HF does not automatically activate the PLT on SG/STMIX	Manually activate PLT HF via Gateway Manager after RLC is completed.
PRB000058886	OSFOURK-21963	During ADP GENDB the commands executed are SWU	V11R0.22
	OSFOURK-27087	Transferring V11 R0 RLC package via SWS functionality in V10 R1 Assistant Software Manager does not work.	Download the RLC package from SWS manually and upload into Assistant Software Manager
	OSFOURK-27514	Update from V10 R0.28 to V11 R0.22 (or newer) via RLC package cannot be done together with Loadware Hotfix V11 R0.22.1 (or newer)	Please transfer and activate the V11 R0.22.x loadware Hotfix after the activation of V11 R0.22
	OSFOURK-27166	STMI2/4 Management IP (MIPADR of MANLANIF) on LAN2 not working when IPDA LAN1 is disconnected	Keep LAN1 cable connected
		After an Assistant re-installation it can happen that licensing does not work properly	Call on Platform with root account: /etc/init.d/cla restart

3.3 Restrictions

Tracking Reference	Internal Reference	Summary
	OSFOURK-26718	Secure Trace for HFA, SIP and SRTP is not supported anymore. Please use internal traces instead.
	OSFOURK-26906	Unify Phone - Assistant EMAIL Restore scripts should contain DIMSU allocation Assistant HF1 for V11R0.22 will correct this. V11R0.22 RLC Transfer & Upgrade should be done together with HF1
	OSFOURK-24577	web certificates with key length less than 2048 bit are not supported anymore. Starting with Platform Hotfix V10 R1.42.1 such certificates for Platform Portal or SoftGate will be automatically replaced with the OpenScape 4000 default web certificate during the Update from previous versions. In such case, please import or generate a new web certificate and distribute to Platform and SoftGates/STMIX/Enterprise Gateways.

Tracking Reference	Internal Reference	Summary
		Note that the CSTA (CAPInside) is preconfigured with ATL LAN address 192.0.2.25 which might conflict with existing old CAP installation.
		From V10, TLS1.0/1.1 protocol versions on all TLS services like HFA, https, SIP is obsolete. Clients which don't support a minimum TLS1.2 will not be able to connect e.g. AC-Win V2, Optipoint Phones (both Post M44) in Signalling and Payload encryption operating mode only, will not be able to operate anymore. Options: disable SPE (not recommended) or upgrade to successor products. e.g. AC-WIN SL V3, CP Phones, …
		CSTA - Restriction for UserToUser There is new config entry for cbdriver: ALLOW_UUI_IN_PRIVATE_DATA – To activate this new feature it should be set to '1'. If this entry is missing, then the feature UserToUser is turned off.
		Hosted SBC WAN Interface The usage of the eth2 as SBC WAN Interface is not supported, please select a different free port. VLAN Configuration on SBC WAN interface is not supported in this SW release.
		OSA500 with 4GB RAM is no longer supported starting with V10R1
		From OpenScape 4000 V10 the STMI2 peripheral board is no longer supported. It is recommended to exchange to the newer STMIX.
		From OpenScape 4000 V10 the Optiset – is no longer supported and will not be operational. It is recommended to exchange to CP200 or CP400 TDM. OpenScape PE cannot be used with Device Types "Optiset" for the same reason.
		Manager - Application Flag Trace Watchdog has been deprecated. Flag Trace was introduced to RMX in EV3.0 to allow users to dynamically have a trace starting via code or special selection that would only pertain to the devices involved in a call. The Flag Trace was not really well adopted, because you could also not use it for Problem Ticket escalation i.e. the trace would only start once a device was reached e.g. if you were tracing a phone, then the phone would need to be rung before the trace started and e.g. if there was an incoming CO call to another station who consulted the device, the previous parts of the call would not be recorded. Since the time Flag Trace was introduced, we also have much better other enhancements like: • selmsg…stno or selmsg…pen in AMO TRACS • Filtering for line numbers in Message Doctor# • RMX Trace profiles and PERMTR
		Manager - starting with OpenScape 4000 V10 R1 Manager the "type" used for communication in System Manager is hardcoded to HLO for all systems. HLB is no longer supported.
		Universal Feature Access (UFA-SIP) - Move operation is not permitted for UFA-SIP extensions. Remark: The SIP loadware usage for UFIP stations requires the usage of SIP PENs, but RMX requires HFA PENs to support HFA functionality internally. Due to this double need, SIP PEN have to be chosen by the user while defining a UFIP station and the PENs are converted to HFA PENs in the background.
	OSFOURK-17188	UPS configuration page not available
	OSFOURK-20547	SIP URI dialling: Dial IN via SIP URI string in conference fails if LoadBalancer is used

Tracking Reference	Internal Reference	Summary
		Openstage 10/15/20/30/40/60/80 TDM and CP200/400 TDM phones are not supported on SLMQ and STHC boards - for details and a possible workaround see INF-22-000131
		TSKA graphical support limitation TSKA uses a simulated phone and it is impossible to mimic any local device interaction like add-on units and CPxxx MWI functionality. In addition, the list phone mode has limited functionality with regard to phone displays with more than two lines. The graphical support for TSKA is considered as frozen and no service ticket will be accepted for this usage mode. As an alternative, J-HPT delivered as part of Assistant can be leveraged for IP phone control. Future enhancements to better serve phone serviceability requirements are part of our backlog and will be included in a later release.
	OSFOURK-21195	Assistant/Manager - Only TLS 1.2. is supported for PKI login
	OSFOURK-22724	Multinode recovery-H4K is not supported starting V11R0. In case of Duplex/GSD, execute recovery-H4K on each node
	OSFOURK-22614	In case of SIP-Q trunking, ECDSA is not supported, please use exclusivity only RSA based certificates
	OSFOURK-27272	SWS Settings lost after RLC Upgrade from V10R1.42 **Workaround:** manually configure the SWS settings.

3.3.1 UC Restrictions

See OpenScape UC Application Planning guide

3.3.2 Video Restrictions

Video support for SIP clients V10R1/V11R0
Video improvements are released with the additional Hotfixes:

- RMX: >= V10R1.42.2
- LW: >= V10R1.42.2
- UC: >= V10R4.14.1

The following features are available for the SIP-Clients supported from OpenScape 4000.

- Hold/Retrieve,
- Consultation/Alternate,
- Call-Forwarding,
- Transfer,
- Conferencing,
- Hunt-Group,
- Pickup-Group,
- Second Call,
- SIP-URI dialling
- Call-back

For further details see also:

- OpenScape 4000 , Service Documentation - IP Solutions - SIP Subscriber – Features
- OSMO and UC Release-Notes

Restrictions / Hints in regards of the usage of Video:

- WebRTC / Fusion Client:
    - Video cannot be activated after
        - Handover from Desk-Phone
        - Hold/Retrieve and Consultation/Alternate
        - Group-Feature Pickup-Group
    - Second-Call is answered with video started
    - No Video to OSV (Video capable client OS4K to video capable client OSV / Video to UC Media-Server connected via OSV)
- OSMO:
    - Black Screen after start of video when selecting "Yes, but don't send my video"
    - Video cannot be activated after
        - Hold/Retrieve via UC Application
        - Consultation/Alternate
        - Call Forwarding
    - Direct Video Call: Video needs to be started manually after feature usage.
    - SIP-URI dialling
    - No Video to OSV (Video capable client OS4K to video capable client OSV / Video to UC Media-Server connected via OSV)
    - Hold/Retrieve is not supported if video is used (SMP=YES).

- 3rd party SIP clients:
    - Only the following features are supported with video:
        - Basic Call (including Networking)
        - Video Conference (UC Media-Server)
    - OS-PE Client (SIP): Video not yet released with V10R1 and V11R0
    - General restriction: ASC recording not possible in case UFIP - UFIP call when DMC is active

Configuration hints:
To activate video the CGW and SDAT DMC parameters need to be set the following way:

```
CGWB:
DMCCONN > 0
SMP=YES
SMP4OSV=NO

SDAT: DMCALLWD
```

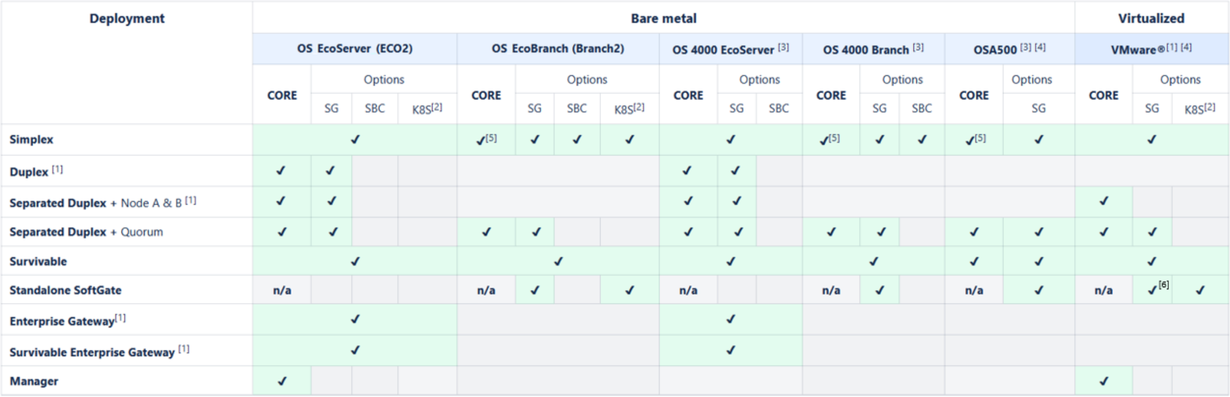
4 Installation and Upgrade / Update

- The SW upgrade of OpenScape 4000 should only be executed by trained (on the current SW Versions) service technicians!

- For every Release Level Complete (RLC) update (Fix Release, Minor Release, Major Release), it is recommended to transfer and activate all available Hot Fixes together with the RLC package. Exception: Update from V10 R0.28 to V11 R0.22 where no loadware hotfix V11 R0.22.x can be added for activation.

4.1 Installation

With V11 R0, the image “OpenScape4000_IMG_V11_R0_22_0” can be used to install ALL deployments (including Manager) listed below:



Deployment	Bare metal																Virtualized		
	OS EcoServer (ECO2)				OS EcoBranch (Branch2)				OS 4000 EcoServer [3]			OS 4000 Branch [3]			OSA500 [3] [4]		VMware® [1] [4]		
	CORE	Options			CORE	Options			CORE	Options		CORE	Options		CORE	Options	CORE	Options	
		SG	SBC	K8S[2]		SG	SBC	K8S[2]		SG	SBC		SG	SBC		SG		SG	K8S[2]
Simplex	✓				✓[5]	✓	✓	✓	✓			✓[5]	✓	✓	✓[5]	✓	✓		
Duplex [1]	✓	✓							✓	✓									
Separated Duplex + Node A & B [1]	✓	✓							✓	✓							✓		
Separated Duplex + Quorum	✓	✓			✓	✓			✓	✓		✓	✓		✓	✓	✓	✓	
Survivable	✓				✓				✓			✓			✓	✓	✓		
Standalone SoftGate	n/a				n/a	✓		✓	n/a			n/a	✓		n/a	✓	n/a	✓[6]	✓
Enterprise Gateway[1]	✓								✓										
Survivable Enterprise Gateway [1]	✓								✓										
Manager	✓																✓		

✓ = supported

n/a = not applicable

[1] Xlink connectivity to Access modules is not supported for VMware deployments, or hosted SoftGates (meaning iSG on Enterprise Gateways and node A or B of Duplex/GSD)

[2] K8S requires 1TB Storage on Bare metal deployments and storage expansion of 50 GB for VMware, depending on workload.

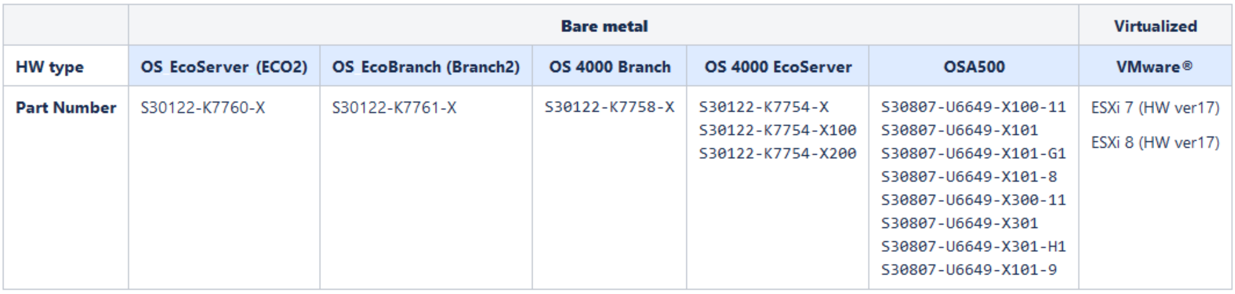
[3] K8S not supported on this HW type

[4] SBC not supported on this HW type

[5] Installation of Simplex without SoftGate on this HW is not released

[6] K8S plus OSEM needs 6 GB RAM on this HW type, so additional 2 GB is needed compared to OVF file

Hardware support and part numbers:



	Bare metal					Virtualized
HW type	**OS EcoServer (ECO2)**	**OS EcoBranch (Branch2)**	**OS 4000 Branch**	**OS 4000 EcoServer**	**OSA500**	**VMware®**
Part Number	S30122-K7760-X	S30122-K7761-X	S30122-K7758-X	S30122-K7754-X S30122-K7754-X100 S30122-K7754-X200	S30807-U6649-X100-11 S30807-U6649-X101 S30807-U6649-X101-G1 S30807-U6649-X101-8 S30807-U6649-X300-11 S30807-U6649-X301 S30807-U6649-X301-H1 S30807-U6649-X101-9	ESXi 7 (HW ver17) ESXi 8 (HW ver17)

4.1.1 Manager installation

Manager installation procedure can be found under chapter 3 in OpenScape 4000 Manager, Installation and Service Manual, Service Documentation

Note:
Starting with OpenScape Manager V10 R1, Appliance SW Installation does not support anymore the co-existing installation of OpenScape Fault Management on same SLES OS.
Consider an external solution as platform, e.g. separate VM in DC.

4.1.2 Manager upgrade

Starting with V10R1, Manager will be delivered as a new deployment of the OpenScape 4000 software. Manager is a SW appliance, meaning the operating system lifecycle is maintained by Unify (same as OpenScape 4000) via Platform HF or RLC.

Migration from older versions must be done using existing Backup & Restore functionality & new installation.
When the restore is performed, the Webmin component should be unchecked to avoid network issues with the old Manager. It is recommended that this part to be configured by manually.

Upgrades from V10R1 and up will be done using the Software Manager (SWM) functionality.

4.1.3 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 Security Checklist “OpenScape 4000 V11, Affiliated Products, Security Checklist“ can be found in service documentation.

4.2 Upgrade / Update / Migration

Migration from earlier versions

The following table describes the requirements for the upgrading to the latest V11R0 – Fix Release

From Minor/Fix Release	Upgrade possible via	Hotfixes, that must be installed prior to upgrade	Reason/Comment
< V8R2	**Not supported**		
V8 R2	RLC[1)]	latest Assistant and Platform Hotfix	
V10 R0	RLC[1)]	latest Assistant Hotfix	
V10R1.42	RLC	latest Assistant Hotfix	

1) All deployments but Manager. For Manager upgrades from V8 R2/V10 R0 see also chapter 4.1.2

The following tables describe the migration options from earlier versions depending on HW/SW

HW information:

Version/HW	HiPath 4000 >= V6 R2.x	OpenScape 4000 >= V7 R2.x	OpenScape 4000 V8R2.22	OpenScape 4000 V10R0	OpenScape 4000 V10R1
VMware	✓ [1]	✓	✓	✓	✓
OS4K EcoServer	x	✓	✓	✓	✓
OS4K Branch	x	x	✓	✓	✓
OS EcoServer	x	x	✓ [2]	✓	✓
OS EcoBranch	x	x	✓ [2]	✓	✓
DSCXL2	✓	✓	✓	✓ [3]	x
DSCXL2+	✓	✓	✓	✓ [3]	x
OSA500	✓	✓	✓	✓	✓ [4]

[1] Only Standalone SoftGate deployment allowed
[2] Support from PLT HF V8R2.22
[3] Only APE deployment allowed
[4] Only OSA500 with 8GB RAM

SW information:

	SW Version / used HW	System	OpenScape4000 >= V8 R2	
SW	Same HW type	HOST	Option 1	Install latest Assistant HF Install latest RMX HF SW Update via HiSPA or SWT&SWA
			Option 2	New SW installation (Including RMX Database Generation e.g. GENDB)
		SurvSG SurvEntGW	Option 1	APE Backup/Restore [1]
			Option 2	Remote Appliance Reinstallation (RAR) [1]
		Standalone SoftGate /Enterprise Gateway	Option 1	GWM - OS Update
			Option 2	Remote Appliance Reinstallation (RAR) [1]
		STMIX	Option 1	GWM - OS Update
	Different HW	HOST [2]	Option 1	New SW installation with RMX Database Generation Hint1: Sam Regen file can be included on the installation media to enable auto GENDB after first installation Hint2: An Assistant logical backup can be used to manually restore previous configurations.

			Option2	Install latest Assistant HF Install latest RMX HF SW Update via HiSPA or SWT& SWA RISO Backup (old HW) RISO Restore (new HW)
		SurvSG	Option 1	New SW installation APE Backup/Restore
			Option 2	RISO Backup (old HW) RISO Restore (new HW)
		Standalone SoftGate	Option 1	New SW installation
			Option 2	RISO Backup (old HW) RISO Restore (new HW)

[1] After the Host was updated; Remote appliance requires minimum version V8 R1.19

[2] For HW changes see Migration Guide

4.3 VMware support

Starting with V11R0, OS4K VM's require minimum virtual hardware version 17, i.e. VMware ESXi 7.0.
To maintain compatibility with VMware ESXi 7.0, the Guest OS in the OVF templates is SLES15.
For details see: https://kb.vmware.com/s/article/55753

In case of first installations, use newly provided OVF templates from the installation media.

Starting with V11R0, OS4K VM's require minimum virtual hardware version 17, resulting in a minimum VMware ESXi 7.0 version.
To maintain compatibility with VMware ESXi 7.0, the Guest OS in the OVF templates is SLES15.
For details see: https://kb.vmware.com/s/article/55753

In case of first installations, use newly provided OVF templates from the installation media.

In case of upgrades from V8R2/V10R0/V10R1, following steps are required for all OS4K deployments (Host system nodes and Standalone/Survivable SoftGates):

- Power off the target VM
- Upgrade VM version from the older version to VM version 17 (ESXi 7.0 and later):

Right click on the desired VM -> Compatibility -> Upgrade VM Compatibility... -> YES -> select "ESXi 7.0 and later" and check that "This VM uses hardware version 17..." is showed below -> click OK to confirm this upgrade.

- Upgrade the Guest OS version to SUSE Linux Enterprise 15 (64-bit):

Right click on the VM -> Edit Settings... -> select the top tab with "VM Options" -> Expand General Options -> Select Guest OS Version from the drop-down: SUSE Linux Enterprise 15 (64-bit) -> click OK to confirm this upgrade.

4.4 Fallback

Fallback procedures are automated as part of the upgrade procedure. If manual fallback is required, the required backups (RISO, Emergency Recovery HD etc) **should be made prior to transferring any upgrade RLC.**

4.5 Special settings and instructions

Not applicable for this release

5 Hardware and Software Compatibility

5.1 Hardware and software compatibility

5.1.1 Minimal HW requirement

SLH or Board	Product Revision	Hardware GA
OpenScape 4000 EcoServer	See chapter 5.1.2 HW / SW Compatibility Matrix	29.05.2015
OSA500a/i	See chapter 5.1.2 HW / SW Compatibility Matrix	16.09.2011
OpenScape 4000 Branch	See chapter 5.1.2 HW / SW Compatibility Matrix	12.12.2016
OpenScape EcoServer (ECO2)	Supported beginning with PLT V10 R0.28.2 PLT V8 R2.22.7	30.09.2020
OpenScape EcoBranch (Branch2)	Supported beginning with PLT V10 R0.28.2 PLT V8 R2.22.7	30.09.2020

Supported HD/SSD

Several serious faults have been reported where unsupported disks are used. Please note only disks below officially ordered via Unify logistic are supported/released and have to be used in order to guarantee system stability and reliability.

Current supported disks are:

EcoServer/Branch SSD	Product Revision / Serial Number	Remarks
Intel® DC S3500 Series	SSDSC2BB240G4 - Serial# BTWL352601xxxx	Unify Part Number - S30122-X8014-X22
Transcend	TS256GSSD420K – Micron NANDs	LTB autumn 2017 No change in Unify part number to Intel SSD
Transcend	TS256GSSD420K UID SSD420K_98 – Sandisk NANDs	LTB autumn 2017 No change in Unify part number to Intel SSD
Transcend	TS256GSSD420K UID SSD420k_196 – Sandisk NANDs	Released 12/2017 No change in Unify part number to Intel SSD
Innodisk	DGS25-B56D81BC1QC-GE1 *Firmware Version: M161225*	Released 2018 No change in Unify part number to Intel SSD
Innodisk	DGS25-B56M71EC3QF-GE1 *Firmware Version: A19307*	Released 2019 No change in Unify part number to Intel SSD
Innodisk	DGS25-B56M71EC3QF-ICC *Firmware Version: A21412*	Released 2021 No change in Unify part number to Intel SSD
Transcend	TS256GSSD452K-ICC 256GB *Firmware Version: 02J0U7JX*	Released Q1/2022 No change in Unify part number to Intel SSD
Transcend	TS1TSSD452K-CC 1TB *Firmware Version: 02J0U7JX*	Released Q1/2022 Unify Part Number - S30122-X8014-X33

Notes:

- There is absolutely no need to migrate existing supported disks to the latest model.
- Only drives supplied from Unify must be used. The reason is we order batches with a fixed set of assembled flash chips. controller and FW version; only these SSDs have passed QA and are supported by Unify.
- For “TS256GSSD420K UID SSD420k_196 - 039A10A” (shipping from spring 2018), with firmware FWP1225CE, the flashing of the activity LED is no longer supported from the manufacturer.

5.1.2 Hardware/Software Compatibility Matrix

HW-Type	Part-Number / Revision	Minimum SW Level	Comment
OSA 500a	S30807-U6649-X100-11	PLT V6 R1.12.2	HW Details: 8 GB with SLMAE
		PLT V6 R2.14.5	
	S30807-U6649-X101	PLT V6 R2.17.1 & RMX V6 R2.17.3	HW Details: 8 GB with SLMAV
		PLT V7 R1.8.2 & RMX V7 R1.8.14	
	S30807-U6649-X101-G1	PLT V6 R2.17.1 & RMX V6 R2.17.3 PLT V7 R1.8.2 & RMX V7 R1.8.14	HW Details: repaired HW with SSD instead of HD
	S30807-U6649-X101-8	PLT V6 R2.17.1 & RMX V6 R2.17.3 PLT V7 R1.8.2 & RMX V7 R1.8.14	HW Details: new HW with SSD
OSA 500i	S30807-U6649-X300-11	PLT V6 R1.12.2 & PLT V6 R2.14.5	HW Details: 8 GB 8 Port SLMAE (Q2331-X100) & STMD3 (Q2332-X)
	S30807-U6649-X301	PLT V6 R2.17.1 & RMX V6 R2.17.3	HW Details: 8 GB
		PLT V7 R1.8.2 & RMX V7 R1.8.14	8 Port SLMAV (Q2338-X1) & STMD3 (Q2332-X)
	S30807-U6649-X301-H1	PLT V6 R2.17.1 & RMX V6 R2.17.3 PLT V7 R1.8.2 & RMX V7 R1.8.14	HW Details: repaired HW with SSD instead of HD
	S30807-U6649-X101-9	PLT V6 R2.17.1 & RMX V6 R2.17.3 PLT V7 R1.8.2 & RMX V7 R1.8.14	HW Details: new HW with SSD
OS 4000 EcoServer	S30122-K7754-X	PLT V7 R1.39.x	8 GB RAM, ordered w/o pluggable SSD and w/o pluggable Power Supply
	S30122-K7754-X100	PLT V7 R1.39.x	8 GB RAM, ordered with pluggable SSD and pluggable AC/DC Power Supply
	S30122-K7754-X200	PLT V7 R1.39.x	8 GB RAM, ordered with pluggable SSD and pluggable DC/DC Power Supply
OS EcoServer (ECO2)	S30122-K7760-X	V10 R0.28.0	16 GB RAM, ordered w/o pluggable SSD and EC/DC Power Supply
OS4k Branch	S30122-K7758-X	PLT V8 R0.x.x	8 GB RAM, ordered w/o pluggable SSD and pluggable w/o Power Supply
			SLMA - Q2346-X

HW-Type	Part-Number / Revision	Minimum SW Level	Comment
OS EcoBranch (Branch2)	S30122-K7761-X	V10 R0.28.0	16 GB RAM, ordered w/o pluggable SSD and EC/DC Power Supply
STMIX	S30810-Q2343-X	PLT V8 R0.x.x	successor of current STMI2/4 board, classical peripheral card.
			only listed here to reflect which SW version is required.
OSA SLA	S30807-U6648-X100	PLT V6 R1.10.0	SLMAE - Q2331-X
	S30807-U6648-X101	RMX V6 R2.16.22	SLMAV - Q2338-X

5.2 Firmware

Not applicable for this release

5.3 Loadware

The included IP Gateway LWs are:
pzksgw50.A9.307
pzksti40.A9.049
pzknci40.A9.048

Note: It is intentional that the LW's version have different suffixes

5.4 Software / Applications

List of SW or SW Product Name	SW Version (e.g. Vx Rm.f.h)
OpenScape 4000 V11 Minor Release 0	V11 R0.22.0
OpenScape 4000 Manager V11 Minor Release 0	V11 R0.22.0

5.4.1 Client Requirements

4K System Release	Assistant/Manager Version	Operating System	Browser Version	Released JRE Versions
V10 R1 V11 R0	V10 R1 V11 R0	Windows 10, 11 and Windows Server 2016, 2019	Edge, Chrome and Firefox are supported browsers. IE might still work with JNLP but no support is offered.	OpenWebStart application (delivered as part of Assistant) is used to run Assistant applications, like CM. The formerly required JRE8 isn't needed anymore

To ensure protection against the latest security vulnerabilities it is always recommended to use the most current System/Assistant version and corresponding HF
Note 1: Windows 32-bit clients are not supported anymore.

5.5 Operating systems

Operating System Name	Operating System Version
Linux	Based on openSUSE Leap 15.5

OpenScape 4000 SW Software Appliance is based on the SUSE Linux Operating System distribution. This means only the necessary OS components are used, which not only streamlines the system - making it more efficient, but also more secure. All software updates (including all updates and Security Patches) will be delivered solely in OpenScape 4000 releases in accordance with the Unify Product SW Lifecycle. It is not allowed to install any additional software, virus scanner or an intrusion detection application.

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 Atos 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!).

5.6.2 Other products

Not applicable for this release

5.6.3 Third-Party products

For more information, please see OpenScape 4000, Installation, Configuration and Migration, Installation Guide, Chapter 1.2. Use of 3rd Party Products

6 Service Information

6.1 Management information base

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

The following MIBs are supported:

Supported MIB's can be downloaded from Assistant under Diagnostics > SNMP/SMTP Configurator or IFMDB.

6.2 License management

This product is certified for the following:

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

The ContractEnd as part of the OpenScape 4000 license prevents future Minor Release upgrades of the OS4K system in case of missing or expired support contract (Hotfix activations are not affected by ContractEnd).

Starting with V10R1, Manager includes a Platform as OS4K does, which comes with its own OS instance and the updating/lifecycle of the OS is managed by OS4K Software (Manager Hotfixes, Platform Hotfixes, RLC images). So, Manager switches from Application model to Appliance model starting with V10 R1.

6.3 Remote serviceability

This product is certified for the following:

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

6.4 Product tooling structure

Main Category	Communication Systems
Product Family	OpenScape4000
Product	OpenScape4000
Product Version	OpenScape4000 V11
Product Item Number	P30152-P1698-P4 P30152-P1698-S1

6.5 Case tracking system

Tickets can be generated and tracked via the Atos 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 Atos 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:

SIP Service Provider (ITSP) Connectivity

For the detailed list of SIP Service Providers and corresponding restrictions - see INF-13-000534
The Wiki from Unify can also be used as reference that contains some of the information provided by the Service INF:
https://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers_on_Enterprise_Platforms.