Atos

Release Notes

Release Notes Version: V1.15, 2024-07-11

Unify OpenScape Desk Phone CP710 CP410 CP210 CP110 HFA V2

Software Version: V2 R0.15.0

☐ 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: N   ECCN: 5D002TSU

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.

Delivered Files

OpenScape Desk Phone CP110

Product Item Number	P30152-P1700-A110-10
File Type	Image
File Name	CP_110_HFA_V2_R0_15_0.img
File Size	17.0 MB
Checksum	6D2A85AD50AC2F1A86C3CFD584F5C5A66BD98091ED774061C55424F0CB874750

OpenScape Desk Phone CP210

Product Item Number	P30152-P1700-A210-10
File Type	Image
File Name	CP_210_ HFA_V2_R0_15_0.img
File Size	18.0 MB
Checksum	1D10FC39A44819681A6ECC98C149BDC17FAF7CE90F2BB8DDD6EE55089E073042

OpenScape Desk Phone CP410

Product Item Number	P30152-P1700-A410-10
File Type	Image
File Name	CP_410_ HFA_V2_R0_15_0.img
File Size	31.2 MB
Checksum	C514B99E394588574794D083FED1FE4A25A7F8E6A726B1650CA557F2024EC6FB

OpenScape Desk Phone CP710

Product Item Number	P30152-P1700-A710-10
File Type	Image
File Name	CP_210_ HFA_V2_R0_15_0.img
File Size	33.0 MB
Checksum	1673284BDE0067C324F6E45A0A12A7B886E8D5CDA80AFB61DE87AE0A73D11B75

Table of Contents

1   History of Change

1.1   Release notes content

Version	Date	Description of changes
1.0	2022-12-09	Release to FT
1.1	2023-01-13	FT Update sw
1.2	2023-01-23	FT Update sw
1.3	2023-02-20	FT Update sw
1.4	2023-04-18	FT Update sw /M3
1.5	2023-05-16	HF Release
1.6	2023-05-19	RN update
1.7	2023-06-26	FT Update sw?M3
1.8	2023-09-19	Fix Release
1.9	2023-09-25	Compatibility matrix update
1.10	2023-10-18	HF Release
1.11	2023-12-14	Fix Release
1.12	2024-1-12	HF Release
1.13	2024-04-03	Fix Release
1.14	2024-04-29	HF Release
1.15	2024-07-11	Fix Release

1.2   Product versions history

Software Version	Production Version	Date	Remarks
V2R0.7.0	V2R0	2022-12-09	
V2R0.7.2	V2R0	2023-01-13	
V2R0.8.0	V2R0	2023-01-23	
V2R0.9.0	V2R0	2023-02-20	
V2R0.10.0	V2R0	2023-04-18	
V2R0.10.2	V2R0	2023-05-16	
V2R0.11.0	V2R0	2023-06-26	
V2R0.12.0	V2R0	2023-09-19	
V2R0.12.1	V2R0	2023-10-18	
V2R0.13.0	V2R0	2023-12-14	
V2R0.13.1	V2R0	2024-1-12	
V2R0.14.0	V2R0	2024-04-03	
V2R0.14.1	V2R0	2024-04-29	
V2R0.15.0	V2R0	2024-07-11	

Note: List of all released software versions since [major] or [minor] software release in SWS.

2   Changes

2.1   Implemented Change Requests / New features

Tracking Reference	Internal Reference	Summary	Released in Version
		USB-A Interface The USB-A interface shall support following functionality (Not applicable to CP110): Bluetooth Headset via USB Dongle CP10 Wifi dongle	V2R0.7.2
		Key module support There shall be up to 4 key modules be supported (not applicable to CP110,CP210). Either paper modules (KM410) or display modules (KM710).	V2R0.7.0
		Gbit LAN 2 Gbit LAN ports are available in CP110	V2R0.3.0
		Security key length 4096bit A minimum key length of 4096bit is available in CP110 in order to secure communication of: SIP, SRTP, https, 802.1x	V2R0.3.0
		Headset interface A headset port with DSHG support is available in CP110 in order to be able to connect a wired headset	V2R0.3.0
		3-line Display New 3-line display support with CP210	V2R0.4.0

2.2   Beta Features

Tracking Reference	Internal Reference	Summary	Released in Version
	DCOA-4101	GC: Limiting the Minimum Ringer Level for CP710 Phones	V2R0.13.0
	DCOA-4468	DSS: Hide calling party number - DLS	V2R0.13.0
	DCOA-4500	WBM: CP-HI Slideshow Format selection	V2R0.13.0

	DCOA-4501	CP-HI User settings Inactivity Slideshow format Best fit to display	V2R0.13.0
	DCOA-4579	Oauth2: Admin configuration data - mobility	V2R0.13.0
	DCOA-4591	Direct network traces	V2R0.13.0
	DCOA-4632	GC: Limiting the Minimum Ringer Level for LO Phones	V2R0.13.0
	DCOA-4634	GC: Limiting the Minimum Ringer Level for Media Control	V2R0.13.0
	DCOA-4651	GC: Limiting the Minimum Ringer Level - DLS	V2R0.13.0
	DCOA-4815	Keep contacts when deleting all conversations - Operation (HFA)	V2R0.13.0

2.3   Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary
PRB000075848	DCO-6255	HFA IFT Munich CP710 H323 connection repeatedly fails (NO AUDIO)
PRB000073394	DCO-6250	CP110 Problem with Deskshare Function
PRB000074622	DCO-6234	Desk Phone CP710 ring roudly (very loud) when receiving MLHG call
PRB000071179	DCO-6187	Half way calls with CP110 phones
PRB000074743	DCO-5933	CP710 phone ringer volume suddenly switched to MAX
PRB000074815	DCO-5871	CP410/CP710 Call Pickup information wrong at phone display
PRB000074505	DCO-5861	CP410 HFA V2R0.13.1 with KM410 (during FT OS4k V11)

	DCO-5805	CP210 HFA ignores the provided VLAN-ID via LLDP-MED
PRB000073701		
	DCO-5792	CPx10 phones V2R0.13.1 are forgetting VLAN-ID after changing to IPv4
PRB000073799		
	DCO-5765	With CP710 HFA there is no/incorrect display of call notifications in SwyxWare context
PRB000072552		
PRB000070990 PRB000075329	DCO-5606	Bad quality audio between CPx10 HFA/SIP and SIP devices

2.4   Resolved Vulnerabilities

Not applicable for this release

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

Not applicable for this release

3.2　Workarounds, Hints

KONFTEL 55W/55Wx/55 feature support

The current official Konftel Unify cable (900103408) does not support the full feature set of the Konftel conference unit is attached to the CP400/CP600(E)/CP700(X). Konftel might introduce a new cable for the full support of the Konftel conference unit down the line; for more information on the availability of such a cable, please contact Konftel directly.

There is a workaround that would enable full support of the current cable when used with CP400/CP600(E)/CP700(X) devices. For this workaround, you have to manually re-cable and switch the middle pins on the connector on the phone side of the official Konftel Unify cable (900103408). Please note that doing this may void the warranty of the cable. Please contact Konftel if you have any further questions.

802.1x

We recommend enabling the support for multicast EAPOL packets on your network devices to avoid issues with the OpenScape Desk Phone CP devices family when using the 802.1x feature.

For specific configuration of multicast, EAPOL packets support, please see your network equipment vendors admin documentation.

Distinctive Ringing

DLS shows all Distinctive Ringing types when phone is connected to a non OpenScape 4000 System, even though the other System supports fewer options. Please use the Local Admin.

3.3　Restrictions

FIPS is currently not supported on CP phones.

DNS SRV Fallback

The configuration option "DNS-SRV fallback on re-register" is not released for OSV/4k environment.

ARP cache Information

Each new cached ARP entry will have a starting timeout between 15 and 45 seconds.

Old entries are garbage collected every 60s.

The ARP entries are not periodically updated (If an IP packet is to be sent to an IP address that does not exist in the ARP table, then an ARP request is sent, and the ARP table is updated with the reply). The intervals are fixed.

"Bad certificate" failure for export contact (Chrome)

The Contact download will be canceled with a "Bad certificate."

The basic problem is Chrome does not trust the WEBM certificates

The reason is a Bug in Chrome (937761 & 939297)

Firefox and IE are working fine

OPUS Codec

Incall automatic switching from wideband to narrowband and vice versa is currently not supported.

Mutual authentication for HTTPS file transfer

For security reasons, the phone will not accept a TLS/SSL renegotiation. If mutual authentication is used against a Microsoft IIS, please check that SSLAlwaysNegoClientCert is enabled on IIS. For more information, please refer to the Microsoft security bulletin MS10-049

http://technet.microsoft.com/en-us/security/bulletin/MS10-049

QDC

Phones generate QDC reports according to QoS protocol version 1.

VLAN

The Device uses 'OptiIpPhone' as a DHCP vendor class identifier. (for the management VLAN and for the voice VLAN)

Remote Tracing

If remote tracing is used, the trace messages sent to the remote Syslog server are not encrypted.

802.1 key size

The Phone, Radius, and root CA certificate can support a max key size of 4096 bits.

Connectivity Check

The Connectivity check must be enabled if you are using transport type TLS; recommended value for check interval is, e.g., 90sec. For transport type, TCP connectivity check should be set to 0sec (disabled). In special network scenarios, it may be useful to enable also TCP connectivity-check (see RQ00034880).

DDNS Name and mobility

Base and the mobile User should be configured with the same "automatic Hostname Type" if you are using the DDNS feature in conjunction with mobility.

Ringer

All default ringer files are included in the SW Bind (Ringer1-6.wav, Harmonize.wav; it is not allowed to deploy ringer files with the same wording as the default files.

Security (WBM) / SSL2 and SSL3

By default, Unify products must configure their SSL/TLS software to
Disable SSL2 (see also RFC 6176) and SSL 3.0 and enable only TLS 1.0 (SSL 3.1) and higher
(Current defined standards are up to TLS 1.2)

NTP Server

For correct time synchronization between the Phone and NTP server, please use a synchronized timeserver. Otherwise, the phone does not accept the transmitted time from the server

DHCP reuse in IPv6 environment

The feature DHCP reuse in the Ipv6 environment is not supported.
The phone needs to be configured to ipV4 only if you want to use the feature.

PC Port

When a PC is connected to the phone PC port, this port is down for a few seconds when the phone is booting.
The second LAN port is designed to connect a desktop PC.
Tagged frames are not supported at the second LAN port.
Mirror Port configuration released for diagnosis only

User PW
Neither the User's telephone number nor display identity is allowed as part of a new password.
Explicitly the following OCMS items are not allowed: 'e164', 'sip-name', 'display-id-Unicode'

Lead Zero (IPV4 Address)
The use of a leading zero on an octet of an IPV4 address is not allowed.
This can lead to a broken service (e.g., DLS, SIP Server, etc.)

DNS
DNS Caching is implemented for the SIP Server/Registrar/Gateway address only.

Ipv6
Stateless Address Autoconfiguration is not supported. Ipv6 is released project-specific only.

MD5 Certificate
Because of security enhancements, Md5 certificates are not supported

Security Scan
A security scan has a significant impact on the performance of the Device. Therefore, we recommend starting security scan's only if the phone is in an idle state. High sporadically, it could be possible that the phone performs a self-restart because of an internal timeout. This behavior is correct and based on the internal software architecture of the Device.

Loop Protection (Cisco switches)
When the pc-port is used in conjunction with Cisco switches, it is strongly recommended to enable bpduguard switch wide using the command "spanning-tree portfast bpduguard default" or to disable "spanning-tree portfast" on all switch ports

PW Expire after (days) configuration
Please note that the date at which a password expires is re-calculated from the date of the last change to the password. Therefore, the PW could be expired immediately after a configuration change.

FTP file Transfer
The phone does not allow special characters for FTP Transfer (original protocol)

QoS
The L2 and L3 priorities need to match each other.
Example configuration based on RFC 2474/2597

Display Error (limited Service NTP)
Since V1R2, the phone shows an error message as soon as the NTP update fails.
In general, most of the phone features are not affected.
Suggested solution: Add a backup NTP server.

jHPT
A dongle file is not necessary to enable access to the HPT interface

The HPT service level access is now protected by
CCE port must be enabled to allow access
A valid TLS connection must be established
A valid Admin password must be provided by the HPT

Group Calls (OSBiz):
Missed Group Calls are not deleted from CP HFA Conversation List if the Originator of the Group Call called that Group, or any member of that Group directly, and such a Call was accepted. If the first (!) Connected Call is a "callback" from a member to the Originator the Group Call is correctly deleted. This is because of an error in OSBiz Signaling for deleting that Group Call entry in case of an Incoming Call.

4 Installation and Upgrade / Update

4.1 Installation

The phone application can be loaded with FTP or HTTPS to the phone, either through the local admin interface, through the Web administration interface, or by the DLS.

For details about the upgrade procedure, please refer to the administration manual.

The SW is signed and will also only accept signed SW. The phone will care about the config parameter (default true) and refuse further downloads of SW that are not signed. Any bind will then need to be signed. The config parameter needs to be changed if a customer wants to install not signed SW as trace/test binds.

Important information for Updates:

- HTTPS download of the software is supported without restriction. Therefore, we recommend using HTTPS Update
- It is recommended to upgrade the phones during low traffic time
- The upgrade can take some minutes. It is strongly recommended to wait until the burning process is finished. (Power off in this situation destroys the phone)
- Please make sure the FTP server and switch are configured with the same LAN Speed and Duplex Mode. Otherwise, it is possible that the download of the software will be interrupted, and the upgrade will fail.
- Please make sure that all old unused 802.1x certificates are deleted before upgrading the phone. Otherwise, it is possible that the deployment will not be finished correctly.
- It is recommended to turn off the traces before the upgrade, especially the ConversationsAPI Tracepoint should not be set to DEBUG on upgrade.

4.1.1 Data and information security

It is mandatory to apply the Security Checklist, so those 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 the latest functionality.

Country-specific regulations must be observed.

The latest version of OpenScape Desk Phone CP710
 can be found under the following link: Fallback
Not applicable for this release

4.2 Special settings and instructions

TLS

WBM ⧠ Network ⧠ Port configuration

The settings for "System Cornet TLS" and System H.225 TLS" should be 4061 and 1300 (Default, or to the ports matching the customer infrastructure. If they are set to "0" the phones will not register.

List of Error Codes

The information located in the following link should be used to find the List of Error Codes
http://wiki.unify.com/wiki/OpenScape_Desk_Phone_CP_FAQ#Error_Codes

5 Hardware and Software Compatibility

5.1 Hardware

Product name	Product Revision	Comment
OpenScape Desk Phone CP110	S30817-S7900-A101	
OpenScape Desk Phone CP210	S30817-S7901-A101	
OpenScape Desk Phone CP410	S30817-S7905-A101	
OpenScape Desk Phone CP710	S30817-S7901-A101	

5.2 Firmware

Not applicable for this release

5.3 Loadware

Not applicable for this release

5.4 Software / Applications

Not applicable for this release

5.5 Operating systems

Not applicable for this release

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.

Product Family	Product	SW Version (e.g. Vx[.y] Rm.f.h)
OpenScape	OpenScape Business	V3R2 FR1 or later
	OpenScape 4000 *1	CP110/CP210/CP410: OS4K V8R2 or later CP710: OS4K V10R1 or later
	DLS *2	V10 R2.3.0 (DLS10R1.626.00) or later
	JHPT	V2 R3.1.22 or later
Web Browser	Microsoft Edge*3	latest version
	Mozilla Firefox	latest version
	Google Chrome	latest version

Notes:
*

*1 Info for usage in OpenScape environments: This overview shows the released components from the phone side, but at the end, the "Common Compatibility Matrix" serves as a binding reference for all compatibility questions.
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/19807d7c-2588-4c6c-ad1b-5f20d509191d

*2 For Limit webserver to TLS 1.2 V7R3.509 or later is necessary

*3 You are advised to clear edge browser cookies before connecting to a device

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!).

5.6.2   Other products

Not applicable for this release

5.6.3   Third-Party Products

Not applicable for this release

6   Service Information

6.1   Management information base

☒ Product forwards SNMP traps according to a MIB

☒ SNMP V2   ☐ SNMP V3

The following MIBs are supported:
- OPENSTAGE-MIB
- QDC-MIB

- SIPPHONE-MIB

6.2 License management

Not applicable for this release

6.3 Remote serviceability

Not applicable for this release

6.4 Product tooling structure

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP110 SIP
Product Version	OpenScape Desk Phone CP110 SIP V2
Product Item #	P30152-P1700-A110-10(V2R0.15.0)

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP210 SIP
Product Version	OpenScape Desk Phone CP210 SIP V2
Product Item #	P30152-P1700-A210-10(V2R0.15.0)

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP410 SIP
Product Version	OpenScape Desk Phone CP410 SIP V2
Product Item #	P30152-P1700-A410-10(V2R0.15.0)

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP710 SIP
Product Version	OpenScape Desk Phone CP710 SIP V2
Product Item #	P30152-P1700-A710-10(V2R0.15.0)

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:
https://wiki.unify.com/wiki