



Release Notes

Release Notes Version:4.4, 2024-06-10

Atos Unify OpenScape Desk Phone CP SIP V1

Software Version: V1 R11.4.0

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: 5D002ENC3

© Copyright 2022, Unify Software and Solution GmbH & Co. KG, All rights reserved.

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.

Atos, the Atos logo, Atos|Syntel are registered trademarks of the Atos group. © 2022 Atos.

Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

Table of Contents

1	HISTORY OF CHANGE	3
1.1	RELEASE NOTES CONTENT.....	3
1.2	PRODUCT VERSIONS HISTORY	3
2	CHANGES	4
2.1	IMPLEMENTED CHANGE REQUESTS / NEW FEATURES.....	4
2.2	BETA FEATURES.....	4
2.3	RESOLVED REPORTED PROBLEMS / SYMPTOMS.....	4
2.4	RESOLVED VULNERABILITIES	5
3	IMPORTANT ISSUES, WORKAROUNDS, HINTS, AND RESTRICTIONS	6
3.1	IMPORTANT ISSUES	6
3.2	WORKAROUNDS, HINTS	6
3.3	RESTRICTIONS.....	6
4	INSTALLATION AND UPGRADE / UPDATE	13
4.1	INSTALLATION.....	13
4.2	SPECIAL SETTINGS AND INSTRUCTIONS	13
5	HARDWARE AND SOFTWARE COMPATIBILITY	14
5.1	HARDWARE.....	14
5.2	FIRMWARE.....	14
5.3	LOADWARE.....	14
5.4	SOFTWARE / APPLICATIONS	14
5.5	OPERATING SYSTEMS	14
5.6	COMPLIANT PRODUCTS	15
6	SERVICE INFORMATION	15
6.1	MANAGEMENT INFORMATION BASE	15
6.2	LICENSE MANAGEMENT	16
6.3	REMOTE SERVICEABILITY	16
6.4	PRODUCT TOOLING STRUCTURE.....	16
6.5	CASE TRACKING SYSTEM.....	17
7	DOCUMENTATION REFERENCE.....	17
8	REFERENCES	18

1 History of Change

1.1 Release notes content

Version	Date	Description of changes
3.0	2022-09-19	Adaption to new RN template and release of FT Version V1R10.1.0
3.1	2022-11-14	release of FT Version V1R10.1.1
3.2	2023-02-10	Release of FR Version V1R10.2.0
3.3	2023-04-04	Release of HF Version V1R10.2.2
3.4	2023-05-19	Release of FR Version V1R10.3.0
3.5	2023-07-07	Release of HF Version V1R10.3.1
3.6	2023-09-06	Release of FR Version V1R10.4.0
3.7	2023-10-06	Release of HF Version V1R10.4.1
4.0	2023-10-30	Release of FT Version V1R11.1.0
4.1	2023-11-24	Release of HF Version V1R11.1.1
4.2	2024-01-19	Release of FR Version V1R11.2.0
4.3	2024-03-26	Release of FR Version V1R11.3.0
4.4	2024-06-10	Release of FR Version V1R11.4.0

1.2 Product versions history

Software Version	Production Version	Date	Remarks
V1R10.1.0	V1R10	2022-09-19	Field trial release V1R10.1.0
V1R10.1.1	V1R10	2022-11-14	Field trial release V1R10.1.1
V1R10.2.0	V1R10	2023-02-10	Fix release V1R10.2.0
V1R10.2.2	V1R10	2023-04-04	Fix release V1R10.2.2
V1R10.3.0	V1R10	2023-05-19	Fix release V1R10.3.0
V1R10.3.1	V1R10	2023-07-07	Fix release V1R10.3.1
V1R10.4.0	V1R10	2023-09-06	Fix release V1R10.4.0
V1R10.4.1	V1R10	2023-10-06	Fix release V1R10.4.1
V1R11.1.0	V1R11	2023-10-30	Field Trial release V1R11.1.0
V1R11.1.1	V1R11	2023-11-24	Field Trial release V1R11.1.1
V1R11.2.0	V1R11	2024-01-19	Fix release V1R11.2.0
V1R11.3.0	V1R11	2024-03-26	Fix release V1R11.3.0
V1R11.4.0	V1R11	2024-06-10	Fix release V1R11.4.0

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

2.2 Beta Features

Tracking Reference	Internal Reference	Summary	Released in Version
	DWE-19972	Increase CP_LO bind sizes	V1R11.3.0

3.1 Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary	Released in Version
PRB000075030	DWE-20065	Calls from secondary line cannot be answered via the headset	V1R11.4.0
PRB000072808	DWE-19948	Issue with Network Call Log with CP205	V1R11.4.0
PRB000074818	DWE-20044	CP600 V1R11.2.0 - D The display is not completely deleted if redirection is deactivated using the program button	V1R11.4.0

7 Important Issues, Workarounds, Hints, and Restrictions

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

Important Issues

7.1 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 if 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.

OPUS Codec

The OPUS codec is now enabled as the default codec with Priority 1 in the audio codec list. As Administrator, you can change the priority of the audio codecs. Please consult the administration documentation for information on how to change the audio codec.

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 vendor's admin documentation.

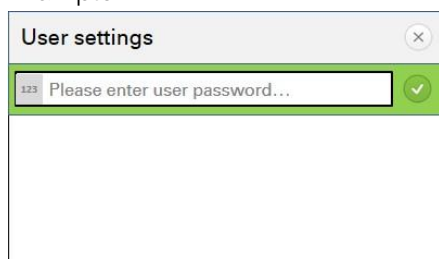
7.2 Restrictions

FIPS is currently not supported on CP phones

CANCEL option

The cancel option is now presented at the top of the screen instead of under the input field

Example:



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 collect 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 updated with the reply). The intervals are fixed

"Bad certificate" failure for export contact (Chrome)

The Contact download will be cancelled with "Bad certificate"

The basic problem is Chrome does not trust the WBM certificates

Reason is a Bug in Chrome (937761 & 939297)

Firefox and I.e., working fine

CAPSLOCK and SHIFT (BT keyboard)

We follow the Linux handling of CAPSLOCK and SHIFT.

WBM Access

Side effects security hardening:

Please delete the cache of your browser if you have problems with the WBM.

You may also need to reset your IE.

Important BT compatibility note:

Factory reset is recommended in the following case:

SW downgrade from the bind V1R5.5.0 or higher to V1R4.X or lower

Reason: possible corruption of trusted/blacklisted BT devices

ICE and DTLS-SRTP

Feature is not supported (please check SRT Key mode is configured to SDES/MIKEY instead of DTLS-SDES)

WBM Screensaver File upload

Screensaver File upload size is limited to 300.000 KB

Bigger files could lead to serious mail functions in case of mobility

OPUS Codec

In call automatic switching from wide band to narrow band and vice versa is currently not supported

Headset and DeskPhone IP

If headsets are used with DeskPhone IP then User-parameter Standard_Ringer/Open_listening should be set to US_mode

Session-Refresh

SIP Session Timer	Session duration	Summary
Enabled	90-3600	SessionRefresh activated, phone is offering to act as refresher (but another peer can claim to be the refresher)
Enabled	0	SessionRefresh activated, phone does not offer to be the refresher (but another peer can push the phone to be the refresher)
Disabled	any	SessionRefresh deactivated (no SessionRefresh handled by the phone – no Supported: timer header)

If the server-type is set to "OS Voice", phone will always respond to an incoming session-refresh Re-INVITE according to OSCAR, no matter whether session-refresh is enabled or not.

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 use 'OptilpPhone' as 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 bit

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 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.mp3, Harmonize.mp3); it is not allowed to deploy ringer files with the same wording as the default files.

Mobility

The mobile user always gets the same set of default ringers after MOB logon.

The basic number of the phone is unavailable during the login period of a mobile user. Equivalent to this the mobile user is unavailable when logged out. It is recommended to use server-based call forwarding features for mobile enabled devices and mobile users.

SIP Backup Server

Whenever a valid SIP backup server address is configured phone will open a port for listening/sending SIP packets to the backup server. If the backup server is not needed in any case it is recommended to configure "0.0.0.0" at the backup server address to totally deactivate the dual-server capabilities.

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 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 Ipv6 environment is not supported.
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 diagnose 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.)

Fixed forwarding

Before changing the fixed forwarding key functionality to any other function than built-in forwarding admin needs to make sure no local forwarding has been activated for that user.

DNS

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

Ipv6

Stateless Address Auto configuration is not supported. Ipv6 is released project specific only.

CP400 Paper label download

An option for downloading key labelling xml (User menu / Phone / Program Keys) is not visible in Internet Explorer. This is working as designed.

Conversation / Mobility

It can take up to one minute until the conversation list is fully synchronized internally. If changes are made to the conversation and MOB is triggered immediately afterwards, the old conversation list may be synchronized, and the changes may be lost.

MD5 Certificate

Because of security enhancements MD5 certificates are not supported

Security Scan

A security scan has a significantly impact on the performance of the device. Therefore, we recommend starting security scan's only if the phone is in 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 configuration change.

FTP file Transfer

Phone does not allow special characters for FTP Transfer (original protocol)

QoS

The L2 and L3 priority needs to match each other.

Example configuration based on RFC 2474/2597

Primary Line FPK

CP700 the primary line can be configured to any of the permanent FPKs or Favorite screen keys

On CP600, "Line" FPK function can be programmed as primary only on Keys 1 to 4 on Key Module 1. All other keys will prohibit primary option for a Line function.

On CP400, "Line" FPK function can be programmed as primary only on built-in keys 1 to 16 (Phone Keys). It is not possible to select Primary option on key modules

On CP200, "Line" FPK function can be programmed as primary for all 4 built-in keys without any restriction.

SIP-TLS connection

If the SIP-TLS connection is set as "Listening" then the current certificate that is used by the phone's web server is also used for the SIP listening port. By default, the web server certificate has weak security and so the default web server certificate should be replaced with a more secure customer-specific certificate (even if the web server or HPT will not be used)

Sidecar

2 sidecars are supported on CP400

4 sidecars are supported on CP600, starting with 2 sidecars external power supply is necessary

4 sidecars are supported on CP700, starting with 2 sidecars external power supply is necessary

4 sidecars are supported on CP700X over PoE (Class 3)

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.

HPT

A dongle file is not necessary to enable access for 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

OpenScape DeskPhone CP periodical connection drops (TCP)

Important Service Information for our OpenScape Desk Phone CP SIP (all SIP versions) is available on G-DMS.

For more information go to <https://www.g-dms.com/>>>INF-17-000137>

Short Description:

An enabled connectivity check in combination with Transport Protocol TCP can lead to a periodical connection drop within the configured connectivity check timeframe.

SIP-TLS connection

If the SIP-TLS connection is set as "Listening" then the current certificate that is used by the phone's web server is also used for the SIP listening port. By default the web server certificate has weak security and so the default web server certificate should be replaced with a more secure customer specific certificate (even if the web server or HPT will not be used)

Signaling and payload performance (re-invite scenario)

Based on the general SIP communication and internal process implementation, a delay can occur in re-invite scenarios with changed SDP information's (up to 400 milliseconds).

This behavior is working as designed. The end device needs a certain time to switch the payload stream.

3.3.2 CP400/600(E)/CP700(X):

Conversation

Conversation matching requires that Canonical settings must be configured and must be correct. Failure to do this will result in misbehavior of the Conversation List.

Exchange

The Exchange server will be handled as master source. Changes on the phone contacts/conversations will not pushed to the Exchange Server.

Voicemail

Voicemail operation depends on the configuration of the "Voicemail number" on the form:
Admin/System/Features/Configuration/General.

If this item is empty, the Main Menu will not show the "Voicemail" item and the user will not see new voicemail indications.

Multi Line Hunt Group (MLHG) and DSS/Line Keys on the same device

In case of the configuration MLHG and DSS/Line keys at the same device an optimized configuration is highly recommended:

Deactivate name update source for LDAP & Signaling

Deactivate 'Busy when Dialing'

Set the visual alert of the DSS/Line key to 'FPK only'

3.3.3 CP20X:

Primary Line FPK

On CP20X, "Line" FPK function can be programmed as Primary for all 4 built-in keys without any restriction.

FPK Call Log

New FPK function "Call Log" should only be programmed on one FPK at any one time. Programming this function on more than one FPK at the same time will result in inconsistent LED indications.

FPK Directory

New FPK function "Directory" should only be programmed on one FPK at any one time. Programming this function on more than one FPK at the same time will result in inconsistent LED indications.

FPK Directory

New FPK Function "Directory" is the only way to see "mode-key" behavior for Phone book on the CP200. Meaning that the only indication that the user sees to show they are looking at Personal or Corporate directory (apart from the screen contents) is the LED on the Directory FPK. If the Directory FPK is not programmed - it will still be possible to program either the "Personal" or "Corporate" (existing) FPK functions and these will still work, taking the user directly to the appropriate screen of the Phone book application...but there will be no LED indication that the user is now in "Directory mode". The Key/LED behavior for the existing "Personal" or "Corporate" FPK functions will NOT be changed into a mode toggle/indicator.

So un-programming the "Directory" FPK is implicitly a statement of intent to either not use the Phone book at all or to accept that there will be no mode toggle or indicator.

8 Installation and Upgrade / Update

8.1 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 config parameter (default true) and refuse further downloads of SW that is not signed. Any bind will then need to be signed. The config parameter needs to be changed if customer wants to install not signed SW like 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 fails.
- 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 of the traces before upgrade, especially the Conversations API Trace point should not be set to DEBUG on upgrade.

8.1.1 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 Desk Phone CP100/20X/400/600/600E/ 700/700X can be found under the following link: <http://apps.gdms.com:8081/techdoc/en/P31003C1010P1010176A9/P31003C1010P1010176A9.pdf> Upgrade / Update / Migration

8.1.2 Fallback

Not applicable for this release

8.2 Special settings and instructions

Not applicable for this release

9 Hardware and Software Compatibility

9.1 Hardware

Product name	Product Revision	Comment
OpenScape Desk Phone CP700X	S30817-S7729-A101-3+	
OpenScape Desk Phone CP700	S30817-S7727-A101-4+	
OpenScape Desk Phone CP600	S30817-S7724-A101-4+	
OpenScape Desk Phone CP600E	S30817-S7723-A101-2+	
OpenScape Desk Phone CP400	S30817-S7722-A101-3+	
OpenScape DeskPhone CP200	S30817-S7720-A101-3+	
OpenScape DeskPhone CP205	S30817-S7721-A101-4+	
OpenScape Desk Phone CP100	S30817-S7730-A101-4+	

9.2 Firmware

Not applicable for this release

9.3 Loadware

Not applicable for this release

9.4 Software / Applications

Not applicable for this release

9.5 Operating systems

Not applicable for this release

9.6 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.l.y Rm.f.h)
OpenScape	OpenScape Voice ¹	V7 Latest version V8 R1.43.2 or later V9 R0.6.2 or later
	OpenScape 4000	OpenScape 4000 V10 R0. or later
	DLS ³	V10 R2.2.0 (HI-DLS10R2.625.00) or later *
	jHPT	V2R4.0.0
Web Browser	Microsoft Internet Explorer	IE11
	Mozilla Firefox	latest version
	Google Chrome	latest version

Notes:

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

³ For EA-Cockpit configuration, V7R3.488.00 or later is necessary
 For Master Source configuration, V7R3.502.00 or later is necessary
 For Limit web server to TLS 1.2 V7R3.509 or later is necessary
 For Mobility logoff switches E/A state V7R3.507 or later is necessary

9.6.1 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!).

9.6.2 Other products

Not applicable for this release

9.6.3 Third-Party products

Not applicable for this release

10 Service Information

10.1 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

10.2 License management

Not applicable for this release

10.3 Remote serviceability

Not applicable for this release

10.4 Product tooling structure

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP100 SIP
Product Version	OpenScape Desk Phone CP100 SIP V1
Product Item #	P30152-P1605-A90-65 (V1 R11.4.0)
Name	CP_100_SIP_V1_R11_4_0.img
Size	27790648 bytes (26 MiB)
Key	SHA256: F17EA630EC95928C741287D487E4A434EAB31871 4F98DB224A6F06520590909C

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP20x SIP
Product Version	OpenScape Desk Phone CP20x SIP V1
Product Item #	P30152-P1605-A100-65 (V1 R11.4.0)
Name	CP_20X_SIP_V1_R11_4_0.img
Size	27963108 bytes (26 MiB)
Key	SHA256: 5BB6D0067964F61AB08A954903A22990CAC625 FACEC38D3CACD2D984ADC6B6D9

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP400 SIP
Product Version	OpenScape Desk Phone CP400 SIP V1
Product Item #	P30152-P1605-A200-65 (V1 R11.4.0)
Key	SHA256: DFD600581BF318A7DE3171A1BC486A14B5C23B9 8461ADF3A8F9A3C16D6D82DB1

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP600 SIP
Product Version	OpenScape Desk Phone CP600 SIP V1
Product Item #	P30152-P1605-A300-65 (V1 R11.4.0)
Key	SHA256: DFD600581BF318A7DE3171A1BC486A14B5C23B9 8461ADF3A8F9A3C16D6D82DB1

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP600E SIP
Product Version	OpenScape Desk Phone CP600E SIP V1
Product Item #	P30152-P1605-A310-65 (V1 R11.4.0)
Key	SHA256: DFD600581BF318A7DE3171A1BC486A14B5C23B9 8461ADF3A8F9A3C16D6D82DB1

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP700 SIP
Product Version	OpenScape Desk Phone CP700 SIP V1
Product Item #	P30152-P1605-400-65 (V1 R11.4.0)
Name	CP_700X_SIP_V1_R11_1_0.img
Size	54511752 bytes (51 MiB)
Key	SHA256: DFD600581BF318A7DE3171A1BC486A14B5C23B9 8461ADF3A8F9A3C16D6D82DB1

Main Category	Clients & Devices
Product Family	OpenScape Desk Phone CP
Product	OpenScape Desk Phone CP700 SIP
Product Version	OpenScape Desk Phone CP700X SIP V1
Product Item #	P30152-P1605-410-65 (V1 R11.4.0)
Key	SHA256: DFD600581BF318A7DE3171A1BC486A14B5C23B9 8461ADF3A8F9A3C16D6D82DB1

10.5 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.

11 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.

12 References

Further related information can be found under the following links:
https://wiki.unify.com/wiki/OpenScape_Desk_Phone_CP