



## Release Notes

Release Notes Version: V2.0

Klaus Kirchberger

**Product Name: *OpenScape Desk Phone CP***

**Product Version: V1**

**Software Release is identified by Version: V1R0.2.0**

Major Release  Minor Release  Fix Release  Hotfix Release

**Production Version:**

System:			
File type	Product Item Number / File name	Size	MD5 checksum
Image	CP400_SIP_V1_R0_2_0.img	36.146 KB	35ea1871869c2b92c6ff507aa1fe56f1
Image	CP600_SIP_V1_R0_2_0.img	36.146 KB	35ea1871869c2b92c6ff507aa1fe56f1

**Export Control Classification Data** AL: N ECCN: 5D002ENC3

Field Trial:  eeQS:  Limited Availability:  General Availability:

### Notice:

This document contains confidential information that is proprietary to Unify Software and Solutions GmbH & Co. KG. No part of its contents may be used, copied, disclosed, or conveyed to any party in any manner whatsoever without prior consent.

**DECLARATION DATE:** Date : 2016-06-24

**DELIVERABLES:** Full Release:  Delta Release:

Copyright © Unify Software and Solutions GmbH & Co. KG, 2016

Mies-van-der-Rohe-Strasse 6, 80807 Munich, Germany

All rights reserved.

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.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

# Table of Contents

<b>1</b>	<b>HISTORY OF CHANGE</b>	<b>3</b>
1.1	RELEASE NOTES HISTORY	3
1.2	PRODUCT VERSION HISTORY	3
<b>2</b>	<b>IMPORTANT INFORMATION</b>	<b>4</b>
2.1	INSTALLATION	4
2.2	UPGRADE / UPDATE	4
2.3	LIST OF ERROR CODES	4
2.4	PORT LIST	4
<b>3</b>	<b>REPORTED PROBLEMS / SYMPTOMS UNDER ANALYSIS</b>	<b>5</b>
<b>4</b>	<b>RESTRICTIONS, WORKAROUNDS AND HINTS</b>	<b>6</b>
4.1	RESTRICTIONS	6
4.1.1	<i>General information</i>	6
4.1.2	<i>New or changed restrictions for this current SW Release</i>	6
4.1.3	<i>Restrictions for this Product-Version</i>	6
4.2	WORKAROUNDS / HINTS	7
4.2.1	<i>New Workarounds / Hints (CP Phone Related)</i>	10
<b>5</b>	<b>CHANGES</b>	<b>11</b>
5.1	NEW IN THIS RELEASE	11
5.2	IMPLEMENTED CHANGE REQUESTS	11
5.3	RESOLVED REPORTED PROBLEMS / SYMPTONS	11
<b>6</b>	<b>HARDWARE AND SOFTWARE COMPATIBILITY</b>	<b>12</b>
6.1	HARDWARE REVISIONS	12
6.2	SOFTWARE RELEASES	12
6.3	COMPLIANT PRODUCTS (COMPATIBILITY MATRIX) <sup>1</sup>	12
<b>7</b>	<b>SERVICE INFORMATION</b>	<b>13</b>
7.1	MANAGEMENT INFORMATION BASE	13
7.2	LICENSE MANAGEMENT	13
7.2.1	<i>Product Structure</i>	13
7.2.2	<i>Diagnostics Structure</i>	13

# 1 History of change

## 1.1 Release notes history

Version	Date	Changes
1.0	2016-06-10	GA release note for SW release V1R0.1.0
2.0	2016-06-24	GA release note for SW release V1R0.2.0

## 1.2 Product version history

List of all released Software Versions since Major Software Release (M3), i.e. all Software Releases in PRISMA/SWS having been released within this Product version:

Software Version (e.g. Vx[.y] Rm.f.h)	Production version (e.g. APS)	Date	Remarks
V1R0.1.0	V1R0	2016-06-10	GA Release
V1R0.2.0	V1R0	2016-06-24	GA Release

## 2 Important Information

### 2.1 Installation

The V1R0.X application can be loaded with FTP or HTTPS to the phone, either through the local user interface or through the Web administration interface or by the DLS. For details about the upgrade procedure please refer to the administration manual.

#### Important information for the installation

- It is recommended to upgrade the phones during a low traffic time.
- The upgrade can take some minutes. (Power off in this situation will not destroys the phone)
- Please make sure that 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 failed.

### 2.2 Upgrade / Update

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.

### 2.3 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/OpenStage\\_SIP\\_FAQ#List\\_of\\_error\\_codes](http://wiki.unify.com/wiki/OpenStage_SIP_FAQ#List_of_error_codes)

### 2.4 Port List

The information located in the following link should be used to find the Port List for the Devices  
<https://hisat.global-intra.net/hisat/>

### 3 Reported Problems / Symptoms under Analysis

GSI-flow Ticket	MR / CQ	Summary	Work-around / Hint
		missing acknowledge/response to DLS after configuration change	
		Security issue: FTP failure of Dongle file leaves port 65532 open when it should be closed	The work around is to correctly configure the FTP parameters when downloading a dongle file
		Security issue: Local Admin does not delete Dongle file from the phone	use the local admin "Disable HPT" option under Maintenance instead or use WEBM instead
		Key Module stuck in upgrade mode	
		first keypress will be ignored (dialing)	
		problem with canonical dialing if feature code will be used	

## 4 Restrictions, Workarounds and Hints

### 4.1 Restrictions

#### 4.1.1 General information

It could be possible that a particular function on the phone is not available. This may be due to reasons that the communications platform does not support this function. Please contact your Unify sales partner for information on how to upgrade.

#### 4.1.2 New or changed restrictions for this current SW Release

##### New Restrictions:

- **Circuit/exchange PW character limitation (WBM)**
  - PW Characters: & " ' ( ) = are currently not supported  
Workaround: configure exchange/circuit locally
- **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

##### Lifted Restrictions:

- **HD Audio**
  - HD Audio indication is missing

#### 4.1.3 Restrictions for this Product-Version

- **DLS-Restrictions**
  - Some parameter are not correctly grayed out in the DLS
- **ICE and DTLS-SRTP**
  - Feature is not supported (please check SRT Key mode is configured to **SDES/MIKEY** instead of DTLS-SDES)
- **Mobility**
  - Not released in conjunction with Exchange
  - Not released in conjunction with Circuit (Beta feature)
  - Cross MOB is not allowed (OpenStage / CP Phone)
- **Cloud Deployment**
  - Cloud Deployment is not released
- **Circuit**
  - Circuit is released as Beta feature only
  - the local conversation model is not more available in case of circuit integration

## 4.2 Workarounds / Hints

- **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	
Enabled	90-3600	SessionRefresh activated, phone is offering to act as refresher (but other peer can claim to be the refresher)
Enabled	0	SessionRefresh activated, phone does not offer to be the refresher (but other 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>

- **LAN Switch**

Device\* phone is designed to be connected to a LAN switch. Therefore only use switches in the LAN to which the Device\* is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- **QDC**

Phones generate QDC reports according to QoS protocol version 1.

- The **web pages** of the phone can be accessed using the following URL:

**Fehler! Hyperlink-Referenz ungültig.** Ip address>

- The Device use ‘OptilpPhone’ as **DHCP vendor class identifier**. (for the management VLAN and for the voice VLAN)

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

- For the **802.1x certificates** there are some restrictions regarding the key size.

The Phone certificate has a max key size of 2048 bytes.

The radius and root CA certificates have a max key size of 4096 bytes.

- The **Connectivity check** must be enabled if you are using transport type **TLS**, recommended value for check interval is e.g. 40sec. 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).

- 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**.

- **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.

- **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 like the default files.

- **Mobility**

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

- **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 released.  
Phone needs to be configured to ipv4 only if you want to use the feature.

- **PC Port**

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

- **User PW**

Neither the User's telephone number or display identity are 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 (eg. 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.

- **OpenStage Manager**

No support for OpenStage Manager

- **XML Interface (EA Cockpit,UC App)**

Not supported

- **Video**

Not supported



- **Certificate Key length**

The RSA public and private keys must be created using either 1024 bit or 2048 bit key length. 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 perform 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 switchports
- **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**
  1. 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.
  2. 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
  3. 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**

4 sidecars are supported on CP400/600  
CP600 from 2 sidecars external power supply is necessary  
CP400 from 3 sidecars external power supply is necessary

## 4.2.1 New Workarounds / Hints (CP Phone Related)

- **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 phone contacts/conversations will not be pushed to the Exchange Server.
- **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)
- **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.

## 5 Changes

### 5.1 New in this release

### 5.2 Implemented change requests

Epic	Feature	Details
<b>V1R0.1.0</b>		
DWE-146	Conversations	Introduction of the <b>Conversation</b> concept. Connected Calls List, Contacts (ldap and Exchange) and Call log combines into single list of items on the Deskphone Display.
DWE-477	Bluetooth	The new Bluetooth technology used in CP600 will contain the latest BT V4.1 standard with the low energy (LE) extensions and advanced feature set.
DWE-4371	Exchange	Acquiring contacts on the phone from an Exchange server (e.g. Microsoft Outlook)
DWE-1072	Ldap	Enhances LDAP functionality eg: Dynamic call related LDAP lookup. If number of an call is not found in the local conversation information, the phone will perform an LDAP search using the number and dynamically create conversation based on the LDAP search result.
DWE-2997	My Features	The Features screen is intended to provide the status of currently available DSS (Direct Station Select) and Multiline/keyset lines when it is not possible to show such a status directly for a key that represents and controls the line (i.e. for WE4 without a KM).

### 5.3 Resolved Reported Problems / Symptons

GSI-flow Ticket	MR / CQ	Summary
		Network Problems CP400

## 6 Hardware and software compatibility

### 6.1 Hardware revisions

Product “long” name	Product Revision	Comments
OpenScape Desk Phone CP400	S30817-S7722-A101-3+	OpenScape Desk Phone CP400 Black
OpenScape Desk Phone CP600	S30817-S7724-A101-4+	OpenScape Desk Phone CP600 Black

### 6.2 Software releases

Product	Software Version	Release Date <sup>1</sup>	G-DMS Note
OpenScape Desk Phone CP400	V1R0.2.0	2016-06-24	
OpenScape Desk Phone CP600	V1R0.2.0	2016-06-24	

### 6.3 Compliant products (compatibility matrix)<sup>1</sup>

Hardware and software products that have been tested together with the phone, including third-party products, are listed in the following table, which also includes the respective versions required to use with the current OpenScape Voice Server software and the location of their respective Release Notes in G-DMS.

Product Family	Product	SW Version (e.g. Vx[y] Rm.f.h)
Openscape	OpenScape Voice <sup>1</sup>	V7 Latest version V8 R1.43.2 or later V9 R0.6.2 or later
	DLS	V7 R3.15.0 (HI-DLS7R3.455.00) or later
	JHPT	V2R3.1.0
Web Browser	Microsoft Internet Explorer	IE8, IE9, IE10 and IE11
	Mozilla Firefox	latest version
	Google Chrome	latest version

**Notes:**

<sup>1</sup> **Info for usage in OpenScape Voice solution environments: This overview shows the released components from phone side but at the end the “OSV Compatibility Matrix” serves as binding reference for all compatibility questions. Stored on G-DMS**

## 7 Service information

### 7.1 Management information base

Product forwards SNMP traps according to a MIB:

The following MIBs are supported:

- OPENSTAGE-MIB
- QDC-MIB
- SIPPHONE-MIB

### 7.2 License management

This product is certified for the following:

CLS:     CSC:     Other Licensing:  If you are using others, please describe below:

#### 7.2.1 Product Structure

Structure in G-DMS / SWS	OpenScape Desk Phone CP400
Main Category	Clients & Devices
Product Family	OpenScape Desk Phone
Product	OpenScape Desk Phone CP400 SIP
Product Version	OpenScape Desk Phone CP400 SIP V1.0
Product Item #	V1 R0.2.0

Structure in G-DMS / SWS	OpenScape Desk Phone CP600
Main Category	Clients & Devices
Product Family	OpenScape Desk Phone
Product	OpenScape Desk Phone CP600 SIP
Product Version	OpenScape Desk Phone CP600 SIP V1.0
Product Item #	V1 R0.2.0

#### 7.2.2 Diagnostics Structure

Structure in Case Tracking System ICTS	OpenScape Desk Phone CP400
Product Family	Clients & Devices
Product Group	WORKPOINT CLIENTS
Product Type	OpenScape Desk Phone CP400 SIP
Product Version	V1
Software Version	V1 R0.2.0

Structure in Case Tracking System ICTS	OpenScape Desk Phone CP600
--	----------------------------

Product Family	Clients & Devices
Product Group	WORKPOINT CLIENTS
Product Type	OpenScape Desk Phone CP600 SIP
Product Version	V1
Software Version	V1 R0.2.0