unify

Release Notes

Release Notes Version: *V13.0*

Product Name: *OpenStage/DeskPhone IP SIP*

Product Version: *V3*

Software Release is identified by Version: *V3R5.13.0*

Major Release □ **Minor Release** □ **Fix Release** ☒ **Hotfix Release** □

Production Version:

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 : 2019-02-27

DELIVERABLES: **Full Release:** ☒ **Delta Release:** □

System:			
File type	Product Item Number / File name	Size	MD5 checksum
Image	OS15_SIP_V3_R5_13_0.img	14.906 KB	376cd29a4de2a7d736e79f292a6b333e
Image	OS40_SIP_V3_R5_13_0.img	14.906 KB	376cd29a4de2a7d736e79f292a6b333e
Image	DPIP35_SIP_V3_R5_13_0.img	14.906 KB	376cd29a4de2a7d736e79f292a6b333e
Image	DPIP35_Eco_SIP_V3_R5_13_0.img	17.546 KB	cec71ed98998ffd849c9aa83099026fe
Image	OS60_SIP_V3_R5_13_0.img	24.944 KB	6abef7ddd15823688a740a01c1569e15
Image	DPIP55_SIP_V3_R5_13_0.img	24.944 KB	6abef7ddd15823688a740a01c1569e15

Table of Contents

1.1 Release notes history

Version	Date	Changes
1.0	2017-01-13	GA release V3R5.1.0
2.0	2017-03-24	GA release V3R5.3.0
2.1	2017-04-07	HF release V3R5.3.2
3.0	2017-07-07	EEQS release V3R5.5.0
4.0	2017-07-18	EEQS release V3R5.6.0
4.1	2017-07-26	GA release V3R5.6.0
5.0	2017-10-10	EEQS release V3R5.7.0

6.0	2017-11-17	GA release V3R5.8.0
6.1	2017-12-22	HF release V3R5.8.1
6.3	2018-03-14	HF release V3R5.8.2
6.4	2018-04-09	HF release V3R5.8.2 (GA)
6.5	2018-04-27	HF release V3R5.8.4
7.0	2018-07-05	EEQS release V3R5.9.0
8.0	2018-08-28	EEQS release V3R5.11.0
9.0	2018-09-14	GA release V3R5.11.0
10.0	2018-10-08	EEQS release V3R5.12.0
11.0	2018-10-24	GA release V3R5.12.0
12.0	2019-01-21	EEQS release V3R5.13.0
13.0	2019-02-27	GA release V3R5.13.0

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**
V3R5.1.0	V3R5	2017-01-13	GA Release (M3)
V3R5.3.0	V3R5	2017-03-24	GA Release (M3)
V3R5.3.2	V3R5	2017-04-07	HF Release
V3R5.5.0	V3R5	2017-07-07	EEQS Release
V3R5.6.0	V3R5	2017-07-26	GA Release
V3R5.7.0	V3R5	2017-10-10	GA Release
V3R5.8.0	V3R5	2017-11-17	GA Release
V3R5.8.1	V3R5	2017-12-22	HF Release
V3R5.8.2	V3R5	2018-03-14	HF Release
V3R5.8.4	V3R5	2018-04-27	HF Release
V3R5.9.0	V3R5	2018-07-05	EEQS Release
V3R5.11.0	V3R5	2018-08-28	EEQS Release
V3R5.11.0	V3R5	2018-09-14	GA Release
V3R5.12.0	V3R5	2018-10-24	GA Release
V3R5.13.0	V3R5	2019-01-21	EEQS Release
V3R5.13.0	V3R5	2019-02-27	GA Release

2 Important Information

2.1 Installation

The V3R5.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

- Software binds before V2R2.42.0 have a sporadic problem, that the phone has not enough memory to store the loaded SW image when HTTPS is used for file transfer. In this case a reboot is recommended before performing the upgrade.
- It is recommended to upgrade the phones during a 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 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.
- 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.

2.2 Upgrade / Update

When upgrading to V3R3/4 from a version lower than V2R2 it is necessary to upgrade to V2R2 first. If you upgrade directly from V2R0/1 to V3R1 all the stored passwords and certificates will become invalid. For upgrades from V2R0/1 please follow the procedure below, upgrades from V1 are not supported.

For upgrades directly from V2R0/1 to V3R1, the certificates and passwords will be invalid and there is an additional procedure to follow to ensure a smooth upgrade process summarized below:

- Prior to upgrade the phone/DLS need to be set to non-secure mode
- The certificates should be removed
- Upgrade the phone
- Re-install the certificates
- Set user and admin passwords via DLS

Before upgrading please check the correct SIP port settings. The **SIP transport protocol** uses port 5061 for TLS and port 5060 for TCP and UDP. The default port setting is 5060. If TLS is used, the port settings must be changed to 5061.

If Web pages are left open during upgrade (e.g. from V2R2 to V3R1), then it is recommended that the web page is refreshed before use on the new version. Failure to do this could result in corrupted display screens and missing configuration, especially with Microsoft IE8.

In General:

A reboot is recommended before performing the upgrade of the SW.

Since V3R3.24.0 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 older software or other not signed SW like trace/test binds.

2.3 Fallback

Prior to downgrade from V3 to V2 or V1 the phone/DLS need to be set to non-secure mode.

After downgrading from V3 to V2R2, V2R1, V2R0 or V1 a **factory reset** of the OpenStage phone has to be performed.

- User/Admin Passwords

  If a downgrade from this bind to an early bind (lower as V3Rx,i.e. V2R2 or before) is required, then the password will need to be reset via the DLS to gain access to phone menu

- Openstage 15 Gigabit SIP

  A downgrade of Openstage 15 Gigabit SIP phones to a version earlier then V3R1.35.0 is not allowed.
  Caution:
  If Openstage 15 Gigabit phones are operated with lower SW versions than indicated above the LAN interface will be broken.

- Certificates:
  - If a downgrade from this bind to an early bind (V2R2.15.0 or before) is required, then there is an additional procedure to follow to ensure a smooth downgrade process summarized below:
    - Prior to downgrade, the phone/DLS need to be set to non-secure mode.
    - The certificates should be removed
    - You downgrade via FTP
    - You re-install the certificates as normal
  - A downgrade to a bind greater than V2R2.15.0000 would be OK as these version have backwards migration code.

- When a downgrade is done from V3R3.3.0 (or from any version above) to an older version, the passwords and data listed above will be lost and need to be re-configured again (passwords are encrypted in V3R3 but all data is lost on downgrade).
  With inclusion of this change following passwords in the phone are no more appearing as cleartext but encrypted:
  - SNMP Trap community password snmp-trap-pwd
  - QCU Community password qdc-trap-pwd
  - snmp community string for queries snmp-pw
  - LDAP password ldap-pwd
  - Bluetooth pin for pairing bt-pin
  - Diagnostic Traps community string diagnostic-trap-pwd
  - All Download FTP parameters used for manual download (not download by DLS) of files:
    - download phone app
    - download moh
    - download picture clip
    - download logo
    - download ldap template
    - download screen saver
    - download ringer
    - download dongle
  - SIP password for digest authentication - sip-pwd
  - SIP line password for authentication at server - line-sip-pwd-xxx
  - DSS key password for authentication at server - dss-sip-pwd-xxx
  - Send URL Server Password - send-url-passwd-XXX

2.4 Security Considerations

n/a

2.5 Special settings and instructions

2.5.1 Migration from OpenStage HFA to OpenStage SIP

1. Load the SIP software to the phone.
2. Perform a factory reset.
3. Configure the phone as a new SIP device.

For details, please refer to the administration manual.

2.5.2 LAN Migration

When a phone is upgraded from a V2R2-version to V3R3 the protocol-mode remains in IPv4 single stack mode.
When a phone is upgraded from a V3Rx-version to V3R3 the protocol-mode remains in the stack mode configured in V3Rx.

2.5.3 XML Application Migration

When a phone is upgraded from V2 to V3 all XML applications are migrated. This migration is done on the first upgrade only. If the phone is later downgraded to V2 and a new XML application is added, this application is not migrated if the phone is upgraded to V3R0 again. In this case the XML application has to be added again in V3.
When a phone is downgraded from V3 to V2, XML applications created in V3 are not migrated to V2. Applications created in V2 before the phone was upgraded to V3 are still available after the downgrade from V3 to V2.

2.5.4 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

2.5.5 How to: VLAN and Quality of Service Parameter

Due to several requests, misconfiguration issues and a changed behavior of the OpenStage phones in comparison to optiPoint 410/420, the following configuration examples of how VLAN and Quality of Service (QoS) parameters should be configured and the impact these parameters will cause should be considered.

There are two parameters that are relevant for VLAN and QoS:

1.) VLAN ID which is found at the Phone Admin menu via Network → General IP configuration
2.) Layer 2 which is found at the Phone Admin menu via Network → QoS → Service

With the optiPoint 410/420 phones those two parameters were very much linked to each other, which was requested for OpenStage not to be the case. This requirement has been fulfilled as much as possible.
So with OpenStage phones it is possible to activate the VLAN functionality even without having to activate the QoS first. But it is still required to have a VLAN ID configured to activate the QoS Layer 2 at the phone.
For example:

Scenario 1: No QoS Layer 2 and no VLAN is used at the customer.

Configuration:

QoS Layer 2 → OFF
VLAN ID → BLANK

It is extremely important to use a blank VLAN ID and NOT the VLAN ID “0” as this VLAN ID is still something and not nothing as you will see in the next example.

Scenario 2: QoS Layer 2 but no VLAN is used at the customer.

Configuration:

QoS Layer 2 → ON
VLAN ID → 0

In this case the phone will operate in the same network segments as in the previous scenario, but the phone will send out tagged frames with the VLAN ID “0” and the corresponding QoS parameters, defined as Priority tagging in the 802.1q standard.
Attention: Some network components may use the VLAN ID “0” for special purpose, please check with the customers network administrators first, and otherwise use Scenario 1 or 3.

Scenario 3: QoS Layer 2 and VLAN are used at the customer. (Recommended)

Configuration:

QoS Layer 2 → ON
VLAN ID → 2 – 4090

VLAN ID “1” should not be set at the phone as the phone already uses this VLAN ID internally so do not use it. This is a permanent restriction.

Scenario 4: QoS Layer 2 is not used but VLAN is used at the customer

Configuration:

QoS Layer 2 → OFF
VLAN ID → 2 – 4090

VLAN ID “1” should not be set at the phone as the phone already uses this VLAN ID internally so do not use it. This is a permanent restriction.

For scenarios 2 and 3 it is also important to configure the QoS Layer 2 values according to the network environment configuration of the customer. There is no right or wrong value. They are only depended on how the different values are interpreted by the network switches. So do not ask GVS or BLS to give you the right values as that is something the customer’s network administrators have to provide.

3 Reported Problems / Symptoms under Analysis

GSI-flow Ticket	MR / CQ	Summary	Work-around / Hint

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.
e.g. the feature ***Directed pickup*** is only available behind OpenScapeVoice V3.1 or higher

4.1.2 New or changed restrictions/hints for this current SW Release

Lifted restrictions:

New restrictions:

New Hint:

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.

4.1.3 Restrictions for this Product-Version

- Feature ‘DLS Contact me - busy state’ is not supported by DLS V7R1 FR4
- Feature Emergency-calling is not released (not supported at OpenScape Voice)
- **DLS-Restrictions**: Following V3R3-phone-features are not supported yet by DLS V7R1 FR4. Phone-administration has to be done via WEBM or local phonemenu. Support of these features is planned for later DLS versions. Affected features are:
  - Video Step2 (QoS values for video may be set via LLDP-Med)
  - Special Ringer Admin Step-2
  - LDAP search on FPK
  - LDAP encrypted
- **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)
- **Video with Asterisk**
  If video is enabled on phones connected to Asterisk it is necessary to have following Asterisk-patch:
  https://issues.asterisk.org/jira/browse/ASTERISK-19830
  If this patch is not installed on Asterisk, feature video has to be disabled on all phones (which is the default setting).
- **Secure-call-icon with Asterisk**
  Secure-call-icon does not indicate unsecure calls when phone has set Server-type=‘OTHER’
- **Keyset-Phones connected to OpenBranch should have no Terminal-name configured**
  Keyset-Phones which use OpenBranch for Survivability should have no Terminal-name configured. Otherwise in survivability-mode wrong names are displayed in Ringing-state (permanent restriction)
- **Trace file size**
  Due to feature enhancements and CR implementation in OS SIP V3 the configurable trace file size could have an impact on behaviour and stability of the phone. For the moment it is recommended to have the maximum size in the following settings:
  LO phones: **2 MB** trace file size

HI phones: **3 MB** trace file size

- **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.
- **User Interface, language support**
  Some translations are missing in the phone user menu. So some items are displayed in English, even the phone is configured for another language.
- **Ipv6**
  Stateless Address Autoconfiguration is not supported.
  Ipv6 is released **project specific only**.
- **ANAT**
  ANAT-support is released **project specific only**.
- **DNS**
  DNS Caching is implemented for the SIP Server/Registrar/Gateway address only.
- **Bluetooth™ Handsfree Profile (HFP)**
  Only a minimal set of HFP functionality is implemented as listed below.
  - Connection management
  - Phone status information
  - Audio Connection handling
  - Accept an incoming voice call
  - Reject an incoming voice call
  - Terminate a call
  - Audio Connection transfer during an ongoing call
- **Multiline**
  On OpenStage 60/80 the number of Feature Programmable Keys (FPKs) that can be configured as multi line or DSS keys is limited to 30.
  On OpenStage 40 and 15 the number of FPKs that can be configured as multi line or DSS keys is limited to 18.
  On OpenScape DPIP-55G the number of Feature Programmable Keys (FPKs) that can be configured as multi line or DSS keys is limited to 30.
  On OpenScape DPIP-35G and ECO the number of Feature Programmable Keys (FPKs) that can be configured as multi line or DSS keys is limited to 3.
- **Half duplex network**
  Gigabit half duplex mode is not supported.
- **IEEE 802.1x**
  The phone acts as a supplicant only, not as an authenticator for a PC, connected at the second LAN port of the Phone. For IEEE 802.1x authentication including MDA behind Cisco Access Switches, IOS 12.2(40) or later is required.
- **802.1x version**
  Since V3R1 the phone will always answer with ***version 802.1X-2004 (2)***
  (to become standard-compliant)
- **Voice dialing**
  Voice dialing is not released.
- **Phone trace**
  Logging should not be enabled for the following components:
  - Service Framework
  - Service Registry
  - OpenStage client management

  If logging is enabled for these components, the phone becomes very slow.
- **USB memory device**
  Connection of a USB Hub to the phone is not supported.
- **Sidecar Support**
  2 sidecars are supported on OpenStage 40, 60 and 80 and OpenScape DPIP-55 and all keys may be programmed as selected dial, call forwarding, etc.
  - One sidecar is supported on OpenStage 15.
  - The sidecar is not hot pluggable. The phone is required to be completely powered off before the side car can be plugged in
  - Paper key module is allowed on OS 40 and 15 only.

- Mixed configurations of paper module and self-labeling key module are not allowed

- **Bluetooth Headsets and Multiline working**
  When using a Bluetooth headset, incoming calls are only indicated with ringing at the headset for calls on the primary line. Calls to secondary lines will not ring at the headset.
- **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.
- **IPV6 and Video**
  IPv6 is not supported at the moment. Please see the following table for a more detailed explanation:

ID	Protocol Mode	Media IP Mode	Used IP Type	Video Support
1	IPV4 only	IPv4 only	IPv4 used	Audio + Video available
2	IPV6 only	IPV6 only	IPv6 used	Audio only
3	IPv4/IPv6	IPv4 only	IPv4 used	Audio + Video available
4	IPv4/IPv6	IPv6 only	IPv6 used	Audio only
5	IPv4/IPv6	IPv4/IPv6	Dual stack	Video only available over IPv4

- **XML applications**
  Please be aware that each XML application requires more than 7MB of memory.
  Each tab within an application counts as a standalone application. When starting too many applications or applications with a large memory footprint (e.g. a lot of images) the phone might run into high/low memory threshold (Admin pages -> Diagnostics -> Miscellaneous -> Memory Information -> Memory Monitor Config).
- **PC Port**
  PC port connection is down on phone reboots.
  When a PC is connected to the phone PC port, this port is down for a few seconds when the phone is booting.
- **Password for serial port access**
  If the serial port access is protected by a password, this password becomes invalid after a software upgrade. Password needs to be reseted via DLS or serial-console (in unprotected mode)
  Please follow the procedure below to assign a new password after the software upgrade:
    - Set the access control for the serial port to ‘No password’.
    - Use the command ‘passwd’ via serial port to set a new password.
    - Set the access control for the serial port to ‘Password required’.
- **Mobility**
  User mobility is released with the following restrictions:
  - Mobility is not released in conjunction with OS Manager
  - A mobile user that is logged on V3R1 cannot logon to a V2R2 phone
  - Since V2R1 all default ringer files are available for a logged in mobile user.
    The mobile user always gets the same set of default ringers. If the user is on a WP HI and deletes one of the default ringers using OSM then it will only be deleted for the duration of that mobile session, and the “deleted” files will appear again at the next logon
  - local phonebook for HI- and LO-phones is not compatible
- **Video**
  Video is only released between Openstage/OpenScape DPIP devices
- **HPT**
  A dongle file is not more necessary to enable access for HPT interface The HPT service level access is now protected by
  1. CCE port must be enabled to allow access
  2. A valid TLS connection must be established
  3. A valid Admin password must be provided by the HPT
- **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
- **2nd Alert**

2nd Alert is not released in conjunction with mobility and/or distinctive ringing

4.2 Workarounds / Hints

- **USB Device // POE**
  If you change the USB-state from disabled to enabled and connect a USB-device you should request a phone-reboot to update the LLDP Power Values
- **Headset and DeskPhone IP**
  If headsets are used with DeskPhone IP then User-parameter ***Standard_Ringer/Open_listening*** should be set to **US_mode** (which is the default value on DeskPhone IP and OS40-US)
- **Feature CallForwarding-on-call-type**
  For new V3R3 feature CF-on-call-type it is necessary to use OpenScape Voice V7R1 FR4
- **OpenStage Manager V3R3**
  OSM V3R3.1.0 or higher is needed to connect to V3R3 phones. Older OSM-versions will not work anymore
- **Session-Refresh**: the phone configuration has changed in V3 in regards to **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)

  Furthermore, to prevent upgrade/downgrade issues (change in configuration):
  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.
- **Secure-call-icons and Video**
  When secure calls are used and video is enabled but no camera is connected at both parties, **the call is a secure call and the secure icon is displayed during the call.**
- **Configuration settings for video-feature**
  If a phone with version V2R2 or V3R0 is upgraded to a version V3R1.X or higher the default settings for video are OFF in Admin- and User-settings
  To enable video generally in admin-menu change
  Admin/System/Features/Feature_access/Video_calls from **Disallow** to **Allow**
  To enable for video in user-menu change
  User/configuration/Video_call/Video_on from **No** to **Yes**
- **Dual Registration / Backup Registration**
  If phone is configured with SIP transport-protocol TLS then SIP backup transport protocol TCP is not working. UDP need to be used in this case for backup protocol.
- **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
- The **SIP transport protocol** uses port 5061 for TLS and port 5060 for TCP and UDP. The default port setting is 5060. If TLS is used, the port settings must be changed to 5061.
- **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 serios malfunctions in the hub and in the whole network.
  QoS Monitoring
  V3 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>
  Access via HTTP is not supported. HTTPS has to be used.
- The Device use 'OptiIpPhone' as **DHCP vendor class identifier**. Unlike the optiPoint 410/420 the Openstage/OpenScape DPIP use this and only this vendor class identifier for the management VLAN and for the voice VLAN.
- When using **OpenStage Manager**, it is necessary to configure the OpenStage Connection Service such that the Password is the same as the User Password configured on the phone. A password must be configured, it cannot be left blank: first configure a User Password on the phone (in the **User/Security** menu) and then configure the **OpenStage Connection Service** to use the same password.
- The **second LAN port** is designed to connect a desktop PC. Tagged frames are not supported at the second LAN port.
- **Hot Desking Feature Key**
  Not available and also not planned for the future.
- If **remote tracing** is used, the trace messages sent to the remote syslog server are not encrypted.
- 802.1x in conjunction with **Cisco C3560**
  Failure:
  The **Cisco dot1x stack gets jammed** if its dot1x configuration after L1 up was almost finished (there are some Identity Req. and a Success to the port if timeout waiting for an answer "tx-period" is too short) and the phone tries to start the negotiation. The stack hangs in state "UNKNOWN" and isn't recoverable!
  Solution:
  Set on Cisco the **tx-period** from 2 sec. to **5** sec. or more (5 sec. is the default value)
- Sometimes it happens that the Phone does not display a "**Telephony is down (RF 2)**" message. This happens if the OSV is not reachable and the "register timeout" of the phone is not expired. The following two failure screens are known:
  - 1st the user enters a number and press dial. The phone displays a "dialing" message and after a while the message changes to "invalid Number".
  - 2nd if you want to dial a number the dialing popup does not appear and it looks like that the keypad is frozen, but in this case the phone displays a "no outgoing line" message which directly disappears if the user presses another key.
- **Emergency numbers/Phone lock**
  1. Emergency numbers can be configured as follows:
     - Admin->System->Features->Configuration->General->Emergency number (1x).
     - Admin->Local functions->Locality->Canonical settings->Emergency number. (Additional emergency numbers, comma-separated).
     - Using the dial plan.
  2. It is possible to dial the following numbers if the phone is in "locked" state:
     - Number from the field: General->Emergency Number.
     - Numbers from the field: Canonical settings->Emergency number.
     - Numbers flagged as Bypass or Emergency in the dial plan.
  3. It is also possible to press the "Emergency call" option when the phone is locked. In this case the phone automatically dials the number of the "General->Emergency Number" field.
- **802.1x error messages**
  1. Bad Certificate
     - Please check the phone time against the release date of the certificate (main failure is a wrong time on phone).
  2. Certificate Expired
     - Certificate is really expired or the phone time is set to "2036-07-03T12:00:03+00:00".
     - If you have the 2036- failure please set the correct time via NTP.
  3. Unknown CA
     - Missing RootCA-Certifikate.
  4. Certificate Unknown
     - This error always occurs when error 1, 2 or 3 doesn´t occur (for example "Critical Policies").

- Restoring a HFA **USB User Backup** on a SIP phone will lead to a filesystem corruption on the USB stick (and vice versa) Only formatting the USB stick will recover the filesystem.
- **LLDP-MED** should only be used with LLDP enabled network access switches. Old network access switches that don't adhere to the 802.1D-1998 MAC bridging specification appear to be propagating the LLDP multicasts through the subnet.
  The default setting for LLDP MED in V2 R0.3.0 (or later) is "ON". As a result of this, the default for VLAN discovery method is "LLDP-MED Discovered".
- 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. 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).
- 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**.
- **Canonical dial lookup**
  Please use the DLS interface if you want to configure/administrate more than 5 Canonical dial lookup entries (max value: 15).
- **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.
- Since V2 **all default ringer** files are included in the SW Bind (Ringer1-6.wav and Ringer1-6.mp3), it is not allowed to deploy ringer files with the same wording like the default files.
- **Extended power management via LLDP-MED**
  LLDP-MED offers a possibility to exchange extended power information between the network switch and the phone via the "Power management TLV".
  Power over Ethernet class detection (see IEEE 802.3-2008 section two) only allows for a rough determination of the actual power consumption of the device. With the help of the LLDP-MED "Power management TLV", the phone and the network switch are capable of a more fine-grained determination of power the device really needs.
  If your switch is not capable of extended power management via LLDP-MED and you encounter any inconsistency in the Power over Ethernet class identified by the network switch and the devices predefined power class, use the following procedure:
  In case Power over Ethernet used only:
  - unplug the device from the Power over Ethernet switch
  - wait 15 seconds
  - plug the device into the Power over Ethernet switch
  Now the phone and the network switch will correctly negotiate the power the switch needs to supply
- **Power supply unit & Power over Ethernet**
  A parallel connection to a Power Supply Unit (PSU) and a Power over Ethernet switch is not supported by the phone.
- **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
- **Cloud Deployment**
  The Phone will always ask for a Cloud Deployment PIN if no DLS Server will be delivered via DHCP and no DLS/Server/registrar is configured on the phone (eg. after factory reset)
- **Certificate Key length**

When generating certificates to be used with Phone Version V3R0 or later , the RSA public and private keys must be created using either 1024 bit or 2048 bit key length. When upgrading from V2Rx to V3Rx if the certificates used for V2Rx use a RSA key length less than 1024bit, then the certificates used in the phone and in servers that connect using secure connections with the phone must be replaced.

- **Certificate encryption**
  Because of security enhancements Md5 certificates are not more supported/allowed in since V3R0
- **Certificate name constraints**
  The SLL version from the phone (0.9.8) does NOT support checking name constraints. Use Certificates that do not specify the unsupported extension.
- **TLS connection**
  In V3R3 a SipStack upgrade introduced RFC 5746 TLS renegotiation (Global Unify goal)
  Therefore TLS with a non RFC 5746 compatible product is not more possible.

  > **Hint:** Up from V3R3.11.1 a Workaround is implemented - "allow non-RFC5746-renegotiation" if the SIP server validation is set to "NONE". This Workaround is only temporary, until configurable Settings are implemented in all needed solution components.
  > **Update Hint:** Up from V3R3.24.0 the temporary Workaround is no more available. The behaves of the phone could be set via the TLS renegotiation parameter "Secure (RFC5646)" or "Insecure allowed"
- **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.
- **Background Color**
  Since V3R1 the background color for skin "Crystal Sea" on Openstage 60 is #E7E7E7 instead of #BDBDBD
- **In case of mobility functionality usage during upgrade from V2 to V3 certain feature availability can get lost**
  because of the new functionality in V3 to enable/disable feature availability in case of an upgrade to V3 a special handling is requested if mobility functionality is used.
- **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
- **"Security file" upload**
  Since V3 the DLS will automatically download the security log file from the device.
  This could lead into an increased traffic on the network and DLS.
  Since V3R1.43.0 these upload can be deactivated via DLS (and only via DLS) by changing the security log file percentage to 0 (these option currently called save immediately in the DLS)
- **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
- **HPT**
  Since V3R3 HPT will only work with transport type "TLS"
- **Geolocation**
  Geolocation is activated by default
  Activated Geolocation with Transport protocol UPD could lead to problems (register/invite will be dropped from the network because it is to large)

L3 Voice: EF (Expedited Forwarding)	L2 Priority: 5
L3 Video: AF41 (Assured Forwarding 41)	L2 Priority: 4
L3 Signalling: AF31 (-"- 31)	L2 Priority: 3

- **LAN port 100Mb fixed speed Setting and EEE combination**
  When using a fixed speed setting of 100Mbps configured at the port on the Network Switch and on the LAN port of the phone, to avoid LI1 at the phone the Network switch must be configured with EEE (Energy Efficient Ethernet) disabled
- **HW Mains Power connections**
  Due to differences between DPIP 35G Eco and Openstage / DPIP power circuits, when a DPIP 35G Eco phone is powered from a mains power supply, then the power supply MUST ONLY be used to power a single DPIP 35G Eco phone. If a power supply is connected to two phones DPIP 35G Eco and an Openstage phone than both phones will be DAMAGED

Attention:

- Please ensure, that the **Auto-Answer flag** is **enabled**, if the user works via CSTA (e.g. OpenScape WebClient).
- **Important:** Since V2R1.X **all** default ringtones on OpenStage 15/20/20E and 40 are changed. All old default ringer files will be overwritten with a SW update to V2R1.X or later.

  How to restore the old ringer files:
  - download the old Ringer files from SWS
  - delete the new ringer files from phone
  - deploy the new ringer files with a **different naming** (don´t use then same labeling like the default ringer files)

# ----------- Begin of Service-Info-------------------#

Service Bulletin INF 13 000367:

UC clients attempting to answer calls receive a message stating “The requested task could not be accomplished” after OpenStage F/W is upgraded to version 3.1.43.0 or higher

OpenStage F/W version 3.1.43.0 and above, has a correction of an error which was incorrectly causing calls to be Auto-Answered on the OpenStage devices when CTI Allow Auto-Answer function was disabled. This resulted in users (without headsets) complaining that their phones would enter hands free mode.

The correct OpenStage behaviors for CTI “Allow Auto-Answer” are:

Enabled - The OpenStage device answers all CTI calls automatically without a user performing an additional physical action on the OpenStage device itself. The OpenStage automatically answers and the parties are connected via hands free or headset.

Disabled - The OpenStage device rings until the user performs one of the following actions:

Lift the handset
Press the alerting line key (keyset only)
Invoke the Answer option via the OK button

When configuring Unified Communications (UC) for a subscriber CTI Allow Auto-Answer should be enabled on the phone device (as documented) but this cannot be enforced at the time of provisioning as the associated device may not exist. Prior to OpenStage FW Version 3.1.43, this had resulted in the possibility of some UC subscribers with either Fusion or Web clients being erroneously able to Auto Answer an incoming call from the answer button on the client without taking any action on the Openstage device itself. When their OpenStage is upgraded to FW Version 3.1.43.0 or later, this incorrect behavior will no longer occur and will result in a message starting “The requested task could not be accomplished” being presented to the client.

For details please have a look at the following document:

https://www.g-dms.com/livelink/livelink.exe/view/INF-13-000367

# ----------- End of Service-Info-------------------#

4.2.1 New LLDP-MED Power Values

Based on previous reports from several customers, the Versions V3 R3.36.1 and later for the OpenStage and OpenScape Desk Phone IP include changed LLDP-MED Power Values.
The previously used values for LLDP-MED were based on average power consumption during normal operation. This has led to incidents in some specific scenarios that some switches had reported that the phone was drawing more power as it had previously requested. Based on switch configuration, vendor and type this could have caused a Power cut off from the network switch which resulted in a reboot of the phone.
The new LLDP-MED Power values are based on the maximum we determined during measurements in development with all LEDs active, maximum Backlight, Ringer on Maximum volume and so on. For some configurations the new values are higher than before. Those measurements and also the reported values from the phone do not take into account the power loss on the used cable. This is nothing the phone can include in the reported values as they are depending on the quality and length of the used cable. It is the responsibility of the Power over Ethernet switch to consider this for the actual reservation of power.
This change of the LLDP-MED Power values does not actually increase the power usage of the phone. It is still drawing the same power as before in every scenario, so the average Power usage and Power cost as reported in the sales information does not change. It is only to take into account several uncommon scenarios that could have lead to more power drawn as previously requested.
It can however have an impact on the amount of phones that could be connected to the same network Power over Ethernet switch, please check the Power Budget of these switches as the Power Budget might be based on the LLDP-MED Power values.

5 Changes

5.1 New in this release

5.2 Implemented change requests

CR-Number	JIRA	Summary
RQ00034575		Support of video Step-2
RQ00032450		Call Indication E/A Cockpit
RQ00037440		OpenStage SSL/TLS secure connection to CCE interface
RQ00034908		Ringer per line
RQ00032219		Local phonebook on WP LO supporting user mobility
RQ00031396		Emergency Calling
RQ00036303		OpenStage: Commonality with Desk Phone IP
RQ00030623		LDAP on 2-line-phones
RQ00032512		Local phonebook on 2-line-phones
RQ00035916		Special Ringer Admin Step-2
RQ00035633		Delete entry from journal when called back
RQ00034370		Ringer On/Off Toggle
RQ00036820		LDAP simple (nickname) search
RQ00036843		LDAP search on FPK
RQ00037010		LDAP search after invocation of consultation/transfer
RQ00037073		LDAP encrypted
RQ00034223		Upgrade Linux kernel to V3.0.9
RQ00032855		DLS Contact me - busy state
RQ00036453		Welsh Language - Step-2
RQ00034954		Redirect-Server Authentication
RQ00036000		Call Forward on call type
RQ00025179		New Design for Call list in XML applications
RQ00033872		XML Applications: XML Table Enhancements
RQ00033855		Call View in focus after make call from XML Application
RQ00033879		XML Application switch off phone cache for XML pages
RQ00032856		XML Applications Event to Server when user enters Application Tab
RQ00030576		Dialling out when residing in an application / mode
RQ00031944		Improvement of Asterisk BLF function
RQ00033853		BLF – Display local identity instead of BLF label
RQ00036565		Deactivation of Serial Port
RQ00035070		Rebranding
RQ00036896		Downgrade protection against RV binds
		V3R3.11.0
RQ00037590		PoE enhancement for SIP
		V3R3.11.4
RQ00037025		Beep ringer option (Openstage Beep Tone)

CR-Number	JIRA	Summary
		V3R3.17.0
RQ00037457		Volume Indicator (SIP)
RQ0003226		FIPs 140-2 configurability
RQ00037392		Lack of forwarding information in WP_LO call log
RQ00033386		WBM access prohibited when no user PW set
RQ00034904		E/A config - Intercom calls on secondary lines
RQ00038098		Bluetooth HFP missing functionality
RQ00033969		WP LO: boot loader update needs to be implemented using SP291_MCH_U-BOOT_140313
RQ00038283		Devices SIP-TLS (Implementation)
		V3R3.24.0
RQ00038345		Desktop phones: Support of RFC5746
RQ00032543		Signed software bind
RQ00036008		DLS Secure Mode easier deployment
RQ00037680		LDAP server authentication
RQ00037945		Mutual TLS support
		V3R3.32.0
RQ00036619		DLS Overload
RQ00037540		Extend volume ranger lower
RQ00038394		OSM on WP_LO
RQ00038352		Mobility during phone lock
RQ00038768		OPENSSL update
		V3R3.36.0
RQ00038527		Support Basque (North Spain) language
		V3R3.40.0
RQ00038171		TLS 1.2 (SIP)
		V3R4.4.0
		Group pickup tone beep: volume has been increased and tone will be repeated every 15 seconds (non configurable)
RQ00039650		New company name
RQ00039112		Enhance OpenScape Desk Phone conference feature
RQ00039135		cyclic ring tone/alert for group-pickup
RQ00039157		Group Pick-up tone is to low
RQ00039455		Increased OSV Pickup tone
		V3R4.5.0
		Group pickup tone beep: volume has been decreased
		V3R4.9.0
RQ00040180		Restore Pickup Tone Settings
		V3R4.10.1
		Support a non-Keyset phone being monitored by a DSS key
		V3R5.1.0
		OpenSSL Upgrade
		reduction of Cut-through delay (payload delay improvement)
		V3R5.3.0
		Remove dongle key dependence

CR-Number	JIRA	Summary
		V3R5.8.0
		Legal information available from WEBM
		Enhance Hold reminder delay timer range
		V3R5.12.0
		Emergency ringer: Fixed ringer volume

5.3 Resolved Reported Problems / Symptons

GSI-flow Ticket	MR / CQ	Summary
		DELAY between RE-INVITE and 200 OK Response
		Device does not follow configured SDP negotiation config after offer less re-invite
		device does not reset some QOS values
		Phones are not able to register using TLS and the IP of SIP-SM (
		Device reports an empty contact-me uri during software deployment and P&P
		CVE-2018-10902, CVE-2018-18386, CVE-2018-17972, CVE-2014-8121, CVE-2017-15671, CVE-2017-17052, CVE-2018-1000001, CVE-2018-6485, CVE-2018-18559, CVE-2018-12233, CVE-2018-10840, CVE-2018-12633,CVE-2018-9384,CVE-2018-11506,CVE-2018-5814,CVE-2016-10723,CVE-2018-10853,CVE-2018-11508,CVE-2018-1000204

6 Hardware and software compatibility

6.1 Hardware revisions

6.1.1 Client

Product “long” name	Product Revision	Comments
OpenStage 15 SIP	S30817-S7401-A501-5+	OpenStage 15 SIP ice blue
	S30817-S7401-A503-2+	OpenStage 15 SIP lava
OpenStage 15 G SIP	S30817-S7401-C501-1+	OpenStage 15 GigaBit SIP ice blue
	S30817-S7401-C503-1	OpenStage 15 GigaBit SIP lava
OpenStage 40 SIP	S30817-S7402-A101-20+	OpenStage 40 SIP ice blue
	S30817-S7402-A103-2+	OpenStage 40 SIP lava
OpenStage 40G SIP	S30817-S7402-C101-9+	OpenStage 40 GigaBit SIP ice blue
	S30817-S7402-C103-3+	OpenStage 40 GigaBit SIP lava
OpenStage 40 US SIP	S30817-S7402-A303-4+	OpenStage 40 US SIP
OpenStage 40G US SIP	S30817-S7402-C303-4+	OpenStage 40 GigaBit US SIP
OpenStage 60 SIP	S30817-S7403-A101-15+	OpenStage 60 SIP ice blue
	S30817-S7403-A103-2+	OpenStage 60 SIP lava
OpenStage 60G SIP	S30817-S7403-C101-5+	OpenStage 60 GigaBit SIP ice blue
	S30817-S7403-C103-3+	OpenStage 60 GigaBit SIP lava
OpenScape DPIP 35G SIP	S30817-S7701-A107+	OpenScape Desk Phone IP 35
OpenScape DPIP IP 35G ECO SIP	S30817-S7710-A107-6+	OpenScape Desk Phone IP 35G Eco
OpenScape DPIP IP 35G ECO SIP	S30817-S7710-A307-6+	OpenScape Desk Phone IP 35G Eco (with icons)
OpenScape DPIP 55G SIP	S30817-S7702-A107+	OpenScape Desk Phone IP 55

6.1.2 USB Video cameras

The information located in the following link should be used to determine which cameras are recommended for use with the phones.
http://wiki.unify.com/wiki/Video_Telephony_for_OpenStage_SIP_60/80
Connecting of unsupported USB cameras is not allowed and could leads into unexpected phone behaviors.

6.1.3 Phone Hardware Changes and necessary Software Versions

The information located in the following link should be used to find the phone hardware changes and minimum necessary software versions of your telephone.
http://wiki.unify.com/wiki/OpenStage_Hardware_Changes_and_Necessary_Software_Versions

6.2 Compliant products (compatibility matrix) [1]

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**	V7R1.51.03+ V8R1.44.01+ V9R0.06.02+
	OSBiz [3]	V2 RX
	DLS [2]	V6R1 CV127.05 or later V7R0 CV218 or later V7R1 CV 312 or later V7R3.459.00 or later
	OpenStage Manager [2]	V3R3.3.0
	HUSIM Phone Tester (HPT)	V2R3.0.2 or later
Web Browser	**Microsoft Internet Explorer**	IE8, IE9, IE10 and IE11
	Mozilla Firefox	latest version
	Google Chrome	latest version

Notes:
[1] ***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***
[2] ***For full support of the new features introduced by phone Version a corresponding Version is required, 35 Eco is not supported until DLS V7R2***
[3] ***released with restrictions (for details please have a look at the OSBiz Release Note)***

7 Service information

7.1 Management information base

Product forwards SNMP traps according to a MIB: ☒

The following MIBs are supported:

- OPENSTAGEPHONE-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: