

Release Notes

System Software 10.2.7

Content

1	Release 10.2.7 Patch 2	2
1.1	Changes	2
2	Release 10.2.7 Patch 1	2
2.1	Error corrections	2
3	Release 10.2.7.100	2
3.1	New Functions	2
3.2	Changes	2
3.3	Error corrections	3

Release Notes describe news and changes in a release for each of the devices for which the release is available. Therefore, they may contain information that is not relevant to your device. If necessary, refer to the data sheet of your device to find out which functions it supports.

1 Release 10.2.7 Patch 2

1.1 Changes

- **Security Update!**

Port-Releases / Firewall policies: In earlier versions of our software, ports for the HTTP (port 80) and HTTPS (port 443) services were opened as port ranges of ten addresses (80-89 and 440-449, respectively). This affected both the configuration of port forwarding and the use of the "Internet" service group when configuring firewall policies.

These port ranges are reset to the default ports by an update to Release 10.2.7 Patch 2. New configurations only use the default ports.

If you need to open the affected port ranges for these services, you have to reconfigure them via the configuration interface. You will find the corresponding settings in the **NAT /Firewall** wizard or in the **Network > NAT** and **Firewall > Policies** menus.

For a better overview, released ports are now displayed in the overview of configured port releases.

If you have not set up port forwarding for the HTTP or HTTPS services in the configuration of your device and have not used the "Internet" service group of the firewall, you are not affected by this possible security problem.

2 Release 10.2.7 Patch 1

2.1 Error corrections

- **System - No IP address obtained (#3726):** After an update to System Software 10.2.7.100, it could happen that devices connected an external modem or gateway that were to obtain an IP address via DHCP did not receive an address if NAT was activated on the corresponding interface.

3 Release 10.2.7.100

3.1 New Functions

- **Support of the LTE stick Huawei E3372h-153:** The stick is now fully supported and displayed with correct information in the GUI.

3.2 Changes

- **Changed VoIP settings for QSC:** The spin-off of QSC's VoIP services to Plusnet GmbH results in changes to the domains to be used for a VoIP

account. The new domains have been incorporated into the corresponding VoIP profiles. Information on the changes can be found in the following document: https://tp.plusnet.de/e/497781/-118546-Domainliste-1-1904-pdf/prgw4/208265821?h=5wrJODsmZwZJs7sZg_Zs51scS4BGV6pXsls_EQmn-Y0 .

- **Key extension T600:** The function "Parking and Retrieval" can be configured via the GUI.
- **Default number in MGW mode:** When operating as a media gateway, the first configured telephone number is now set as the default number during initial configuration. If the configuration is converted from operation as PBX, the settings made there are adopted.
- **SCEP - Certificate renewal:** If a renewal of existing certificates is carried out via SCEP, an error could occur if there were changes in the certificates (e.g. to the subject name). The existing certificates could then not be replaced by the new ones.

System software 10.2.7 changes the behavior so that the existing certificate chain is removed before the SCEP procedure is carried out. After successful completion, it is completely replaced with the new certificates, provided that the number of certificates in the chain has not changed. If an error occurs during the procedure (e.g. an interruption of the Internet connection), the new certificate chain is not saved and the device tries to perform the procedure until it is successful.

In this state after an error, there are no valid certificates for the corresponding connection available on the device - IPsec connections cannot be established and rekeying cannot be performed. After restarting the device in this state, the old certificates are temporarily restored until the SCEP procedure restarts.

This behavior is controlled by the new MIB variable

CertMgmtAutoCleanup. After the software update it has the value *true*. If set to *false*, the old behavior is restored, where the certificate chain is replaced without prior cleanup.

- **System – be.SDx compatibility (W2003ac access points):** The upcoming availability of our cloud management solution requires several changes to be made to the behavior of **W2003ac** access points.
- **New option "ipBootpRelayOutboundPort":** Determines the UDP source port to be used for the DHCP relay functionality. If set to *bootpc* (1), the common source port 68 (BOOTP client) will be used. If set to *bootps* (2) source port 67 (BOOTP server) will be used instead.

3.3 Error corrections

- **be.IP 4isdn - Restart (#2645, 3088, 3222):** There could be repeated panics of the **be.IP 4isdn**.
- **IPsec Client - No DNS (#1866):** It could happen that no DNS server was assigned to a connection via the IPsec Client and therefore no name resolution could take place.

- **System - No voice mail server after reboot / flash memory not recognized (#2280, 3241):** It could happen that the additional flash memory of the device was not recognized after a reboot. Among other things, this could lead to the VMS no longer being available.
- **Phones - update by time not possible (#2401):** It was not possible to update the system software of a DECT150 after a certain time had elapsed. The update started immediately.
- **Telephony - Connection aborted in case of multiple forwarding (#3152):** In case of multiple forwarding at a Corporate Voice Solutions connection of Deutsche Telekom, the call was aborted after the second forwarding.
- **Telephony - Problem with retrieval in Open Inquiry (#3249):** If a call was placed in Open Inquiry, it could possibly only be retrieved if automatic outside line access was not configured.
- **System - Memory loss (#3284):** If the DynDNS service could not successfully propagate the current IP address of the device, a gradual loss of memory occurred.
- **SIP - Call Aborts (#3374, 3377):** VoIP calls could be aborted on several occasions. This mainly affected connections with a very short re-registration timeout.
- **Telephony - CLIP No Screening with CPBX phone (#3390):** When using a CPBX, the SIP headers were parsed in such a way that the desired number was not displayed with CLIP No Screening.
- **WLAN Controller- Double SSID not possible (#3427):** It was not possible to use an SSID more than once, this was prevented by the GUI. The use of the same SSID can now be configured via the extended configuration menus of the WLAN controller.