Release Notes
System Software 10.2.3

Content

1 Release 10.2.3.100 (Final)

1.1 Notes

- **Please note that not all new functions are available in all our products. Refer to the data sheet of your device for information about its scope of functions.**
- **A new function may be provided for different devices at different times.**

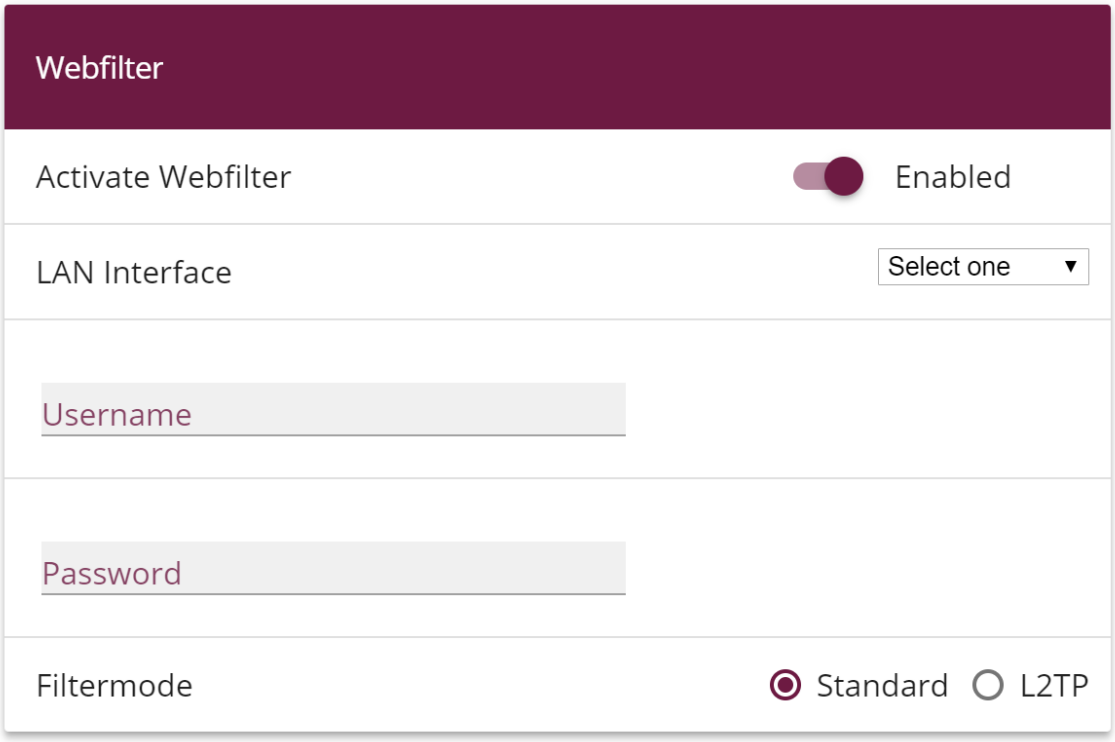
1.2 New functions

1.2.1 Web Filter Wizard

To filter unwanted traffic and protect your network against malicious web pages, the bintec elmeg web filter can now be set up using a simple configuration wizard.

Note that you must purchase a license to operate the web filter. Information can be found at http://www.bintec-elmeg.com/produkte/software/software/webfilter/.

In the **Assistant> Web Filter** menu, the configuration of DNS servers, firewall and DynDNS settings can be made based on only few choices:



After selecting the LAN interface, all clients in this network segment are automatically taken over into the filtering, since all DNS requests from this segment are routed to the DNS servers of the Web filter. If you select an interface for which no DHCP server has yet been set up, you can enter the range of IP addresses to be filtered yourself.

Clients on other networks are exempt from filtering - their DNS requests are still routed to the default DNS servers.

The configuration of the filtering itself takes place in the web application under https://webfilter.bintec-elmeg.com. Username and password will be provided upon registration.

When filtering, you can choose between two modes:

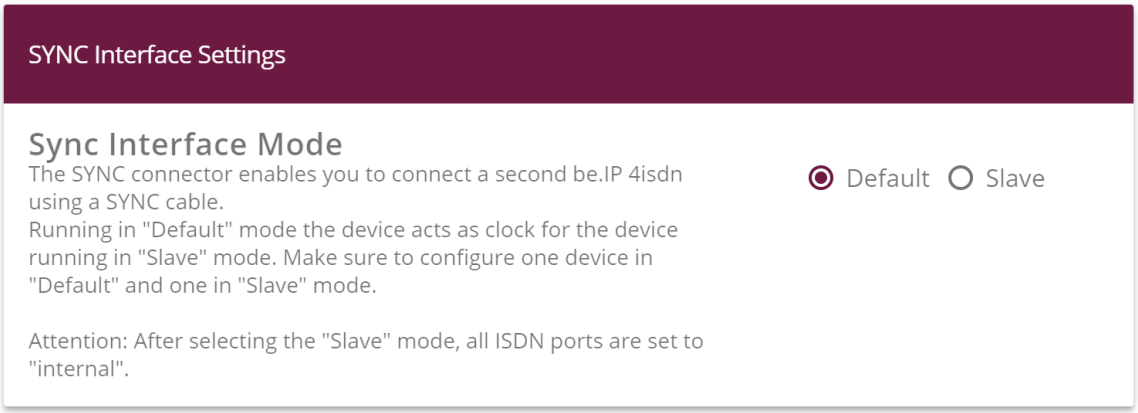
• *Default*: In this mode, your device sends requests to the Web Filter through the public IP address of its router. The filter identifies the configuration to be used based on this address.

• *L2TP*: This mode allows you to operate the web filter even if your router does not have its own public address. For example, if your Internet service provider carries out so-called "carrier grade NAT" in which several routers in the network of the provider share a public network address.

Note: The option of filtering via an L2TP tunnel is currently not available, but will be made available by the operator of the web filter in the future.

1.2.2 be.IP 4isdn: Synchronization of two devices

In order to access up to eight ISDN ports, two be.IP 4isdn can be connected via the sync connection and a corresponding cable. To prepare for this pairing, you should ensure synchronization of the ISDN clock between the devices. In the menu **Physical Interfaces> ISDN Ports> ISDN Configuration** you can configure devices for operation as a clock generator (*standard*) or a clock receiver (*slave*):



Afterwards you can configure your application. Information about possible use cases can be found in the manual as well as on http://www.bintec-elmeg.com/produkte/all-ip/beip/beip4isdn.

1.2.3 VoIP provider profiles

When setting up your phone lines in the **Assistants> Telephony> Trunks** menu, default provider profiles now simplify the configuration. For some of the most important providers, these profiles ensure that settings (such as the preferred

codecs) are made "in the background" to allow seamless telephony. Profiles are available for both, MSN and DDI connections.

If you create a *user-defined* trunk, the settings are based on a default profile that provides compatibility with different providers. Even in this case, you only have to make a few settings yourself.

1.2.4 "Partial Rerouting"

Some service providers require the function of partial rerouting for call forwarding in the exchange. Due to the diversion in the exchange, no voice channels are allocated at the originally called subscriber. Partial Rerouting must be supported and activated by the provider. The configuration then takes place in the PABX of the customer.

No special configuration is required for the activation of partial routing.

1.2.5 Extension of Domain Forwarding

When configuring domain forwarding in the **Local Services> DNS** menu, you can now use the source interface of the DNS request as a forwarding criterion for both types of forwarding (to an interface or to specific DNS servers).

This allows routing DNS requests from different network segments to different DNS servers. In this way you can, e.g., route requests from a guest network to a web filtering DNS and filter unwanted content while requests from the corporate network are still routed to the company DNS server or to the DNS server of the Internet service provider.

1.3 Changes

- **be.IP world edition:** The number of access points that can be managed by a WLAN controller license has been increased from six to twelve.
- **L2TP:** To support the web filter, **L2TP** has been added as a tunnel protocol in the **VPN** menu.
- **IPSec - IKEv2 Rekeying**: In order to configure the active rekeying of an IKEv2 SA, you can specify the lifetime percentage that triggers the rekeying in the **VPN> IPSec> Phase 1 Profiles> Create New IKEv2 Profile** menu.

1.4 Error corrections

- **DHCP - Multiple IP addresses not possible via MAC address (# 1494):** It was not possible to statically assign multiple IP addresses to a client with a single MAC address in the GUI.
- **GUI - Missing options in self-configured access (# 1445):** If a profile has been created in the **System Management> Configuration Access> Access Profiles** menu that allows access to the **Global Settings** menu, the menu options **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** were missing.
- **HotSpot - Too high values possible (# 807):** When configuring a HotSpot server, it was possible to specify a very high number of clients for the field **Devices per ticket** (previously **Max. Number of sessions per user**). The maximum number has been reduced to *10*.

- **GUI - VoIP accounts cannot be linked to WAN connection (# 1163 - RTxxx2):** It was not possible to link a VoIP account to a specific location and assign it a specific WAN connection. The corresponding menu was not available.
- **RXL - IPSec traffic aborts (# 1573):** After some time, IPSec connections could discard all packets even though the tunnels were still established.
- **SIP - Call aborted (# 1452 - Media Gateway):** It could happen that a parked call over an SRTP connection was terminated by the exchange when it was resumed.
- **Telephony – Automatic pick-up without MoH (# 1675):** If a team configured automatic pick-up with Music on Hold, the music was not played reliably.
- **IPSec- Panic in rekeying (# 1651):** It could happen that a panic occurred if both sides requested a rekeying of the IKE SA at the same time.
- **SIP - No telephony (# 1577):** After a SIP transmission error, no further SIP data were transferred.
- **SIP Registration issue (# 1480, 1514 - PBX):** Some service providers require the private IP address of a client in order to maintain registration if the public IP address changes. This was not guaranteed until now.
  In addition, problems could occur if the IP addresses contained in the SIP REGISTER and SIP INVITE messages were not the same.
- **System - Bad quality of recorded messages (# 1536):** Recorded audio files (e.g. messages on the answering machine) showed poor recording quality.
- **SIP - Panic (# 1483 - Media Gateway):** There may be sporadic reboots of the device.
- **SIP - Call terminations (# 1464 - PBX):** Calls were not established if SIP messages on the part of the service provider and on the part of a be.IP interfered with each other – e.g., if a SIP UPDATE from the device met a re-INVITE from the remote site.
- **GUI - Bridge mode not supported (# 1557):** For devices operated as a WLAN client, selecting the bridge mode of the corresponding interface was available although this combination is not supported. The corresponding option is no longer be displayed.
- **UMTS/LTE - Incoming SMS interrupts Internet connection (# 1613):** An incoming SMS on a UMTS/LTE interface caused the Internet connection via this interface to be disabled; reconnection required a reboot.
- **SIP - Call misinterpreted (# 1598):** An incoming call to a modem connected to an FXS port resulted in a tone being interpreted as a fax tone. Then a Re-INVITE with T.38 was sent to the provider, and the modem connection was never established.
- **SIP – Incorrect number assumed (# 1516):** If the FROM field of the SIP header contained no "user=phone" information, it could happen that the phone number in the INVITE was not extracted correctly. To work around this, a user name that begins with a "+" is now interpreted as a phone number.