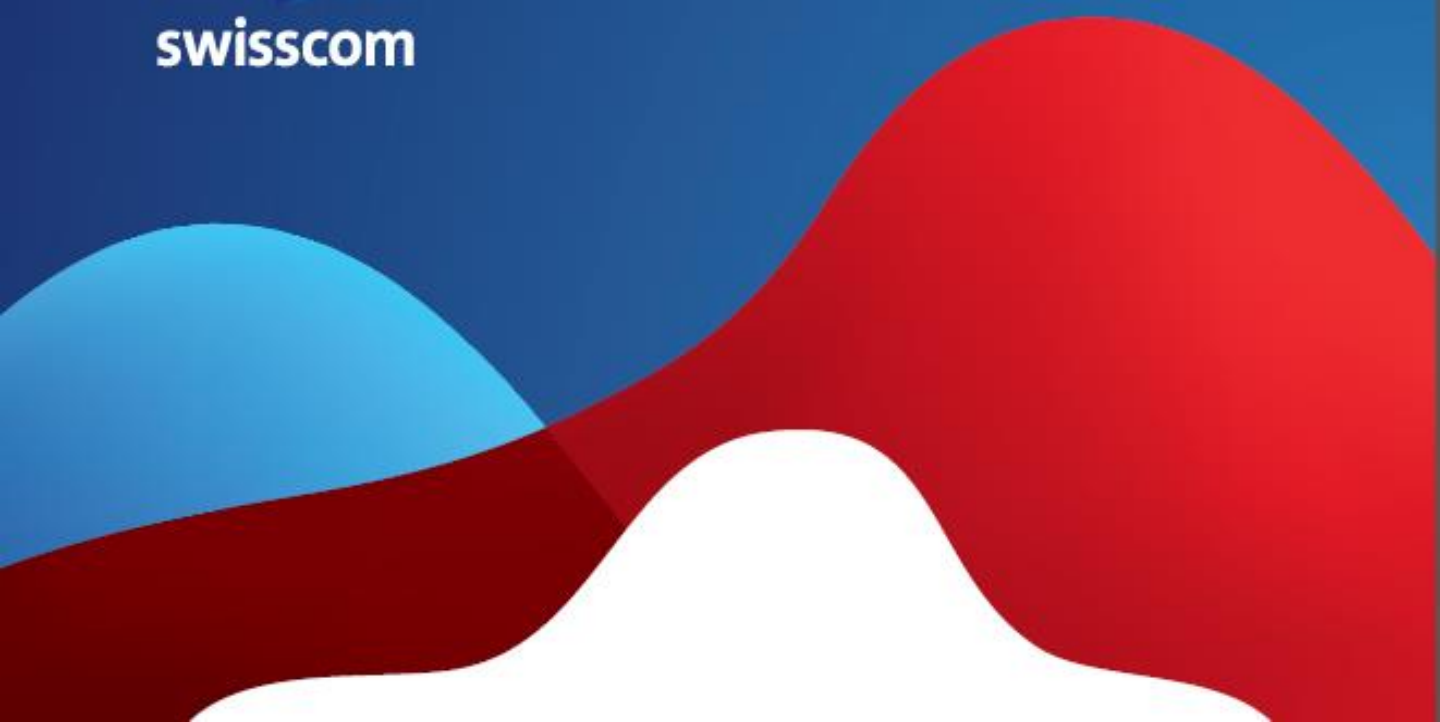
Release Notes older Firmware versions Centro Business 2.0

Centro Business 2.0
Konfigurationsanleitung

Swisscom (Schweiz) AG
KMU
3050 Bern



Router Firmware 9.50.08 / B14+++ (Nov. 2021)

As announced, we have now received a newer firmware, which also solves the ISDN problems (echo & quiet voice). The current firmware rollout will continue with the 9.50.08 version.

Fixed bugs

- When using ISDN telephones, the other party can be heard very quietly.

Router Firmware 9.50.06 / B14++ (Nov. 2021)

Info: In the firmware 9.50.06 there is still a known error when using ISDN telephony (echo or other party is very quiet). Therefore, this firmware is currently not used for InOne SME customers who use VoIP and possibly ISDN. (no automatic firmware update).

Fixed bugs

- With certain ISDN telephones (especially Gigaset), there is an echo heard by the other party
- Sbcon customers who have analog phones connected to the ATA interface do not see caller ID display and missed calls. (CLIP incorrect)
- Customers who use PPP Passthrough sometimes have service restrictions with: VPN, business telephony connection setup, BLF keys. (Negotiation of the MTU size)
- For customers using PPP passthrough WAN reset in the router portal, this leads to a router crash (hardware reset is necessary).
- For customers with MAO BNS & VoIP, the telephone does not ring on "Sammelanschluss" with parallel ringing and the "BLF" does not work (only "Busy Lamp Field List" visible).
- Customers with BNS and DMZ have occasional interruptions which can be temporarily solved with a router restart.

Router Firmware 9.50.04 / B14+ (April 2021)

Fixed bugs

VLAN10 conflict with Enterprise Connect (fiber)

If an "Enterprise Connect S" customer configures a VLAN10 on the LAN port of a fiber optic connection (FTTH & XGS-PON), no Internet connection can be established (conflict on WAN and LAN port with the same VLAN10) Existing BNS installations are nevertheless affected if they subsequently set up a VLAN10 (access) in the LAN.

Router Firmware 9.50.02 / B14 (April 2021)

New features

Disable Ethernet port individually

Ethernet ports can now be completely deactivated individually in the router portal under "Network". This way abusive device connections in the LAN can be suppressed. If a device is connected to a deactivated port, the LED on the Ethernet port will not light up. Please note that Swisscom does not know whether you are using this function in case of support and therefore reports any connection problems.

Monitoring in the router portal for SPAM analysis

If a customer is identified in the Swisscom network by potential SPAM traffic, he is directed into a sandbox process and blocked in case of recurring disregard. We now offer the option of analysing traffic via port 25 and determining which device is triggering it in the router portal under "Analysis" → "Connection Monitoring". You can use this function only if you log in via Superadmin or Techadmin.

Improved security for site-to-site VPN with IKEv2 profile (SHA2-256 & PFS)

With the new firmware, we also support the SHA2-256 hash function with IKEv2. In addition, you can decide in the Peer to Peer VPN settings (IKEv2 Profile) whether you want to work with or without the PFS option (Perfect Forward Secrecy). To the help document.

VPN DH Groups

The VPN now supports multiple DH groups.

VPN Logs in router GUI

Now you can also view the VPN logs in the router GUI, you can find them under Diagnostics -> System Log .

Support of the new USB stick E3372h-320

The firmware also supports the new 4G USB Sitick for Internet backup.

Custom DynDNS provider available

Now we allow to make an individual DynDNS entry in the router portal. In this way we offer high flexibility to the user. However, since the many providers require very individual configurations, the following applies: This is an expert function, Swisscom neither offers help nor provides support! You can find tips and tricks in the help document.

ICMP Redirect

Now you can turn off the ICP Redirect for static routes

New, stricter router password (Admin) requirements

To actively ensure the security of our customer installations, we have decided to tighten the password requirements for the router login. At least 10 characters and at least 1 character each of the following character types:

- Lower case: All lower case letters; so a...z
- Capital letters: All capital letters; so A...Z
- Numbers: All numbers; from 0 to 9
- Special characters @ = + -". * / \ ( ) [ ] { } # % & ? ! € . : , ; $ _(Underscore)
  except ; < > and spaces € £ § ° ö é Ö Ä à ä ç ~ ¿ ¡

Resolved and known errors

resolved = ✓ Known = ✘

	Known since the Firmware version
✓ With certain ISDN telephones (especially Gigaset), there is an echo heard by the other party	9.50.02
✓ Sbcon customers do not see Call number display and missed calls on the analogue telephone interface (ATA) (CLIP incorrect)	9.50.02
✓ Customers who use PPP Passthrough sometimes have service restrictions with: VPN, business telephony connection setup, BLF keys. (Negotiation of the MTU size)	9.50.02
✓ For customers using PPP passthrough WAN reset in the router portal, this leads to a router crash (hardware reset is necessary).	9.50.02
✓ For customers with MAO BNS & VoIP, the telephone does not ring on "Sammelanschluss" with parallel ringing and the "BLF" does not work (only "Busy Lamp Field List" visible).	9.50.02
✓ Customers with BNS and DMZ have occasional interruptions which can be temporarily solved with a router restart.	9.50.02
✓ With certain ISDN telephones (especially Gigaset), an echo occurs when the other party is on the phone.	9.50.02
✓ When using ISDN telephones, the other party can be heard very quietly.	9.50.06

With the new firmware, the DECT driver is updated and delays the availability of services by up to 20 minutes

Known Limitation
The restoration of the Centro Business 2.0 configuration (Backup & Restore), which was generated on an older firmware version, is not possible due to the fundamentally revised data model. It is recommended to create a backup file recurrently on an installation with new firmware. For further information on creating a backup, please refer to the help document.

9.03.xx

Router Firmware 9.04.10 / B 13+++ (Januar 2020)

New features

Download

XGS-PON fibre optic technology.

The new firmware allows the Centro Business 2.0 to be reused on the upcoming XGS-PON technology (March 2020) with a new SFP module.

The customer needs a new SFP module from Swisscom. This allows a surfing speed of max. 1Gbps to be achieved.

Resolved and known errors

resolved = ✓ Known = ✘

	Known since the Firmware version
✘ PPP passthrough mode supports a MTU of 1492 instead of 1500	8.06.08
✘ Various language translation errors in the GUI	9.01.02
✘ Port forwarding is deleted after a WAN reset	8.06.08
✘ Certain traffic from the DMZ to the LAN is not blocked	9.02.12
✘ Selective restoring does not work properly	8.06.08
✓ LAN connections to the DMZ are made with the LAN IP instead of the router WAN IP (ID 3403)	9.03.xx

With the new firmware B13 the DECT driver is updated and delays the availability of the services by up to 20 minutes

Known Limitation

The restoration of the Centro Business 2.0 configuration (Backup & Restore), which was generated on an older firmware version, is not possible due to the fundamentally revised data model. It is recommended to create a backup file recurrently on an installation with new firmware. For further information on creating a backup, please refer to the help document.

9.03.xx

Router Firmware 9.04.06 / B 13++ (November 2019)

Troubleshooting

- Incorrect DMZ routing has been fixed
- "No Audio- Participants don't Hear Each Other" Fixed SIP Calls Issue
- "No Audio Participants Don't Hear Each Other" Fixed Issue via DECT
- Improvement in multicast handling

Router Firmware 9.04.04 / B 13+ (August 2019)

Solved problems

- Sporadic Internet connection problems after firmware update on copper lines
- Sporadic disconnections from ongoing telephone calls (port change)
- Optimization of the telephone connection Establishment (Codec Handling)

Router Firmware 9.04.02 / B 13 (July 2019)

New functions

Support of the "Toolkit for Business" for "Business Internet Services wireless"

With the new firmware, the Centro Business 2.0 Router supports the "Toolkit for Business" for "Business Internet Services wireless". This service increases the mobility of your Internet access and enables business customers to ensure an improved bandwidth even in less developed areas. (via mobile network

Support of the "Toolkit for Business" as Internet failover

With the new firmware, the Centro Business 2.0 router supports not only the existing USB dongle but also the "Toolkit for Business" as a failover (4G)

Support of the DECT Gigaset Repeater HX

With the new firmware, Centro Business 2.0 supports the use of the DECT Gigaset Repeater HX, which will be available in the future. The new firmware supports up to two repeaters and max. 2 HD phones will be connected.

Modernization of VPN encryption

The potential Site to Site VPN connections have been redesigned to provide increased security by supporting the IKEv2 encryption methodology. (So far IKEv1)

Improved list of devices in the router portal

The device list overview in the router portal now offers more detailed information about the network. To the respective connected LAN device is declared via which Ethernet port (1-4) or which WLAN (2.4 / 5.0) it is connected. It also indicates the speed with which the device currently works with the Centro Business 2.0 (LAN). Ethernet becomes 10/100/1000Mb, with WLAN the current down- and up-link speed is displayed. To refresh the information, the page must be reloaded.

Identify IP conflicts in the router portal

The Centro Business 2.0 signals an IP conflict if IP address duplicates are detected in the network. A red warning appears on the overview page and the affected entries are displayed red in the device list. If an IP conflict is detected, please contact your network administrator.

Run local firmware update at night

In order not to interrupt a company's Internet access during office hours, for a manual firmware update, the router portal offers the option to automatically carry out the update the next night (2:00). In this guide we explain how to do the delayed firmware update. Attention! During an interim firmware update, a reboot or a reset of Centro Business 2.0, the pending firmware update will be deleted.

Configure smaller IPv4 subnets than / 24 in LAN

To gain more control over network size, new subnets can now be configured between "/ 8" (16mio IP addresses) to "/ 30" (2 IP addresses). Until now, the smallest option was "/ 24" (254 IP addresses).

Legal functional adjustments

⇨ Further information

Unencrypted WLAN is blocked

With the adjustments to the legislation of the Federal Office for Surveillance, Swisscom must ensure that unauthorized people are not allowed to misuse our customers' WLAN. The WLAN on the Centro Business 2.0 can no longer be broadcast unencrypted.

Stricter WPA2 WLAN password requirements

The following requirements apply when defining a WLAN password: The password must be at least 10 characters long (16 characters or more are recommended) and must contain at least 1 character from the following character types:

- lowercase	All lowercase letters; (a...z)
- capital letters	All capital letters; (A...Z)
- numbers	All numbers; (0 to 9)
- special characters	special characters; @ = + - " * / \ ( ) [ ] { } # % & ? ! € . : , ; $ exept < > and spaces

The character _ (underscore/underscore) is also allowed, but is not assigned to any of the named character types.

Existing "weaker" passwords can still be used despite firmware update, but must meet the requirements with the next change in the router portal. We recommend that you do this proactively.

Renaming the guest WLAN to "separated WLAN"

We call the guest WLAN "separated WLAN" new. By adapting the legislation of the Federal Office for Surveillance, Swisscom must ensure that unauthorized people cannot use our customers' Wi-Fi abusively. Swisscom recommends that all SME customers that their Wi-Fi signals or their passwords no longer be forwarded to unknown parties. Details on the adaptation of the law can be found in the WLAN leaflet of the "Postal and Telecommunications Traffic Monitoring Service".

Router Firmware 9.02.14 (October 2018)

New functions

- None

Bug fixes

- The rare synchronisation issue with the Swisscom network of the Centro Business 2.0 with factory setting (commissioning or after reset) is solved with this firmware. In case of synchronisation issues with firmware 9.02.12, the router can be updated manually via a local device (PC). The process of a manual update is described here (Variant 2 " Firmware Update via the help page")

Known bugs with firmware 9.02.14:

- None

Router Firmware 9.02.12 (June 2018)

The firmware is primarily an improved version of firmware 9.02.06 / 9.02.10 and stabilizes installations using FixIP, port forwarding or DMZ.

All Centro Business 2.0 not yet using firmware 9.02.06 or FixIP, port forwarding or DMZ will be automatically updated to the new version (9.02.12) within the next weeks. However, you can manually update the firmware from the official Centro Business 2.0 help page.

Bug fixes for Upgrades from 9.02.10

- Port forwarding: If port forwarding is used on the Centro Business 2.0 with FixIP, the port forwarding works correctly again after the firmware update and after a router restart.
- DynDNS: The DynDNS service works correctly again after the firmware update and after a router restart.

Known bugs with firmware 9.02.12:

- In rare cases, a router with factory settings (commissioning or after reset) that wants to connect to the Internet via copper technology, cannot synchronise with the Swisscom network. Please contact the SME Hotline.

Router Firmware 9.02.10 (June 2018)

The firmware is primarily an improved version of firmware 9.02.06 and stabilizes installations using FixIP and DMZ.

All Centro Business 2.0 not yet using firmware 9.02.06 or FixIP and DMZ will be automatically updated to the new version (9.02.10) within the next weeks. However, you can manually update the firmware from the official Centro Business 2.0 help page.

Bug fixes for Upgrades from 8.06.08:

- DMZ: The fact that business telephony has registration or connection problems in the "DMZ on Port 1" application case after a PPP interruption or reboot has been solved.
- DMZ: The error that occasionally the DMZ function does not start correctly after a firmware update has been fixed.
- Further stability improvements

Known bugs with firmware 9.02.10:

- DynDNS: The DynDNS service may occasionally be interrupted. As a workaround, the DynDNS option can be deactivated and reactivated in the Router GUI.
- Port forwarding: If port forwarding is used on the Centro Business 2.0 with FixIP, the rules are visible in the router portal but do not work during the firmware update in the same way as during a router restart. The error can be corrected by disabling and re-enabling the port forwarding in the router portal. By avoiding a router restart, you can prevent the error from occurring again.

Router Firmware 9.02.06 (April 2018)

New functions

Support of G.fast

G.fast is a state-of-the-art technology that enables us to massively increase data transfer speeds on the copper fixed network. Expansion of the network has just begun and is continuing all the time. Check available bandwidths.

Support of Premium Call

Valid only for My SME Office and inOne SME Office

Six telephone calls can be made simultaneously if six or more channels are included in the subscription. The two ISDN voice channels can be now deactivated and therefore be available for the DECT telephone base station. The number of simultaneous calls is limited as set out below. Settings can be altered in the router portal under the menu item VoIP/Basic Settings. Changing the existing settings results in a router reboot.

Simultaneous telephone calls for each technology	Number of telephone channels when ISDN telephones in use	Number of telephone channels with ISDN deactivated
Analogue telephony (tel.)	2	2
ISDN telephony (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

Manual DNS server configuration

In the router portal, the manual DNS mode can now be activated under the menu item "Internet Basic Settings" and thus a preferred primary and secondary DNS server can be defined. This function allows you to bypass the newly introduced Internet Guard.

New ‘techadmin’ user role for optimal IT partner customer support

A new ‘techadmin’ role has been created alongside the well known user roles ‘admin’ for local router portal access and ‘superadmin’ for temporary remote access (activated in the Customer Center).

Once approved in the router portal, this role can temporarily access the router portal both locally in the LAN and remotely (only https://). The permanent password can initially only be created by ‘admin’ (customer/owner), who decides whether to make such access available to a trusted partner in order to benefit from optimal, secure support. ‘techadmin’ enjoys the same rights as ‘admin’, apart from the right to see or change the ‘admin’ and ‘techadmin’ router access password

Router remote management in order to configure the WLAN, for example

It is now possible for ‘techadmin’ to carry out various configurations on the Centro Business 2.0 remotely via https:// encryption.

Detailed help documentation

Important

Admin’ must initially create the ‘techadmin’ role with a password in the router portal.
Both ‘admin’ (locally) and ‘superadmin’ (remotely via the Customer Center) can activate temporary ‘techadmin’ remote access by setting the access time (15, 30, 60 mins).
Only one user role can remotely access the router portal at a time.
Permanent remote access has been abolished for security reasons

Procedure for ‘techadmin’ to activate remote access:

1. Activate remote access via the Customer Center and access the router portal with the ‘superadmin’ login
2. Under the menu item ‘Router’, select and save the access time. The ‘superadmin’ session will then be ended.
3. To log in as ‘techadmin’, the existing URL in the browser must be manually changed to https://“WAN-IP“.
4. The login window will be displayed if you type ‘Enter’. Log in with ‘techadmin’ and the password previously set by ‘admin

NAT tables (LAN & DMZ) under Diagnostics (only visible to ‘superadmin’ and ‘techadmin’)

The NAT tables for LAN and DMZ can now be viewed and exported in the router portal under the menu item ‘Diagnostics’. You can therefore identify an active session via the relevant IPs and ports in order to analyse or debug your network. You can find further informationen about how NAT works here.

Bug fixes for Upgrades from 8.06.08:

- The problem with people listening in to calls through handsets connected via DECT and internal call forwarding has been resolved
- Various limitations in the use of IPv6 have been removed
- SBcon telephony connection failures have been corrected
- Centro Business 2.0 configured with IP Passthrough can correctly connect to the Internet after a DSL signal interruption
- Centro Business 2.0 with IP Passthrough without active host configuration, works correctly
- Improved PPP connection with fibre connections
- Various improvements to BNS Service stability
- DNS malpractice, related to the Internet backup function is corrected.

Important recommendation:
Customers who have taken the Internet Backup Stick out of operation due to service restrictions in the past, should reconnect it to the Centro Business 2.0 in order to benefit from the service availability via the mobile network in case of an interruption.

Bug fixes for upgrades from 9.01.04:

- Calls with local SIP credentials via the guest WLAN are no longer supported for security reasons
- For accesses with a fixed IP, port forwarding settings are correctly applied after a WAN reset
- Internal with external conference connections do now work correctly.
- Various connection problems and interruptions (after approx. 15min) in telephony, as well as problems with the BLF display have been fixed.
- Various improvements in connection setup via fibre and DSL, as well as DHCP stability improvements in the local network.
- The automatic WLAN channel selection of the 5gHz band works correctly again
- The DMZ works correctly again after PPP connection interruptions.

Bug fixes for upgrades from 9.02.04:

- The B subscriber can correctly confirm calls with keypad dialing (DTMF)

Known errors with firmware 9.02.06

- DMZ: The DMZ function does not work sporadical after an FW upgrade.
- The error can be corrected by deactivating and reactivating it in the router portal.
- DynDNS: The DynDNS service can be occasionally interrupted. As a workaround, the DynDNS option can be deactivated and reactivated in the router GUI.
- In the case of a PPP session interruption, the business telephony (PBX@HET and SIP phones with Smart Business Connect and InOne SME) behind it may have problems with registration or telephoning in the "DMZ on Port 1" application case. This problem is also present on earlier firmware versions and can be corrected by restarting the router.
- Concerning only firmware intermediate version 9.01.04:
- In the router-portal, if you click "Check for Update" (under "Router-> Firmware), although the router finds the new firmware version 9.02.06, it cannot be installed. The message "Firmware is up to date" is erroneously displayed. Alternatively, the firmware can be selected and installed locally as a file.

Router Firmware 9.02.04 (March 2018)

New functions

Support of G.fast

G.fast is a state-of-the-art technology that enables us to massively increase data transfer speeds on the copper fixed network. Expansion of the network has just begun and is continuing all the time. Check available bandwidths.

Support of Premium Call

Valid only for My SME Office and inOne SME Office

Six telephone calls can be made simultaneously if six or more channels are included in the subscription. The two ISDN voice channels can be now deactivated and therefore be available for the DECT telephone base station. The number of simultaneous calls is limited as set out below. Settings can be altered in the router portal under the menu item VoIP/Basic Settings. Changing the existing settings results in a router reboot.

Simultaneous telephone calls for each technology	Number of telephone channels when ISDN telephones in use	Number of telephone channels with ISDN deactivated
Analogue telephony (tel.)	2	2
ISDN telephony (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

New ‘techadmin’ user role for optimal IT partner customer support

A new ‘techadmin’ role has been created alongside the well known user roles ‘admin’ for local router portal access and ‘superadmin’ for temporary remote access (activated in the Customer Center).

Once approved in the router portal, this role can temporarily access the router portal both locally in the LAN and remotely (only https://). The permanent password can initially only be created by ‘admin’ (customer/owner), who decides whether to make such access available to a trusted partner in order to benefit from optimal, secure support. ‘techadmin’ enjoys the same rights as ‘admin’, apart from the right to see or change the ‘admin’ and ‘techadmin’ router access password.

Router remote management in order to configure the WLAN, for example

It is now possible for ‘techadmin’ to carry out various configurations on the Centro Business 2.0 remotely via https:// encryption.

Important

Admin’ must initially create the ‘techadmin’ role with a password in the router portal.
Both ‘admin’ (locally) and ‘superadmin’ (remotely via the Customer Center) can activate temporary ‘techadmin’ remote access by setting the access time (15, 30, 60 mins).
Only one user role can remotely access the router portal at a time.
Permanent remote access has been abolished for security reasons

Procedure for ‘techadmin’ to activate remote access:

1. Activate remote access via the Customer Center and access the router portal with the ‘superadmin’ login
2. Under the menu item ‘Router’, select and save the access time. The ‘superadmin’ session will then be ended.
3. To log in as ‘techadmin’, the existing URL in the browser must be manually changed to https://“WAN-IP“.
4. The login window will be displayed if you type ‘Enter’. Log in with ‘techadmin’ and the password previously set by ‘admin

NAT tables (LAN & DMZ) under Diagnostics (only visible to ‘superadmin’ and ‘techadmin’)

The NAT tables for LAN and DMZ can now be viewed and exported in the router portal under the menu item ‘Diagnostics’. You can therefore identify an active session via the relevant IPs and ports in order to analyse or debug your network.

Bug fixes

- The problem that used to appear in the interim version 9.01.02 – calls interrupting after 15-30 minutes, using HD-Phone Sarnen and Yealink T45G – has been solved.
- The problem with people listening in to calls through handsets connected via DECT and internal call forwarding has been resolved
- Various limitations in the use of IPv6 have been removed
- SBcon telephony connection failures have been corrected
- Centro Business 2.0 configured with IP Passthrough can correctly connect to the Internet after a DSL signal interruption
- Centro Business 2.0 with IP Passthrough without active host configuration, works correctly
- Improved PPP connection with fiber connections
- DNS malfunction related to Internet Backup function has been corrected
- Various improvements to BNS Service stability

Known errors with firmware 9.02.04

- The automatic channel selection of the 5gHz band does not work correctly. With the firmware 9.01.04, the Centro Business 2.0 always selects channel 36. If the WLAN connection quality is disturbed by many other WLAN signals and generates problems with the Internet connection, it is recommended to manually manipulate the channel in the router portal.
- Concerning only firmware intermediate version 9.01.02: In the router-portal, if you click "Check for Update" (under "Router-> Firmware), although the router finds the new firmware version, it cannot be installed. The message "Firmware is up to date" is erroneously displayed. Alternatively, the firmware can be selected and installed locally as a file. The file can be downloaded from the help page.

Router Firmware 9.01.04 (September 2017)

New functions

Support of G.fast

G.fast is a state-of-the-art technology that enables us to massively increase data transfer speeds on the copper fixed network. Expansion of the network has just begun and is continuing all the time. Check available bandwidths.

Support of Premium Call

Valid only for My SME Office and inOne SME Office

Six telephone calls can be made simultaneously if six or more channels are included in the subscription. The two ISDN voice channels can be now deactivated and therefore be available for the DECT telephone base station. The number of simultaneous calls is limited as set out below. Settings can be altered in the router portal under the menu item VoIP/Basic Settings. Changing the existing settings results in a router reboot.

Simultaneous telephone calls for each technology	Number of telephone channels when ISDN telephones in use	Number of telephone channels with ISDN deactivated
Analogue telephony (tel.)	2	2
ISDN telephony (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

New ‘techadmin’ user role for optimal IT partner customer support

A new ‘techadmin’ role has been created alongside the well known user roles ‘admin’ for local router portal access and ‘superadmin’ for temporary remote access (activated in the Customer Center).

Once approved in the router portal, this role can temporarily access the router portal both locally in the LAN and remotely (only https://). The permanent password can initially only be created by ‘admin’ (customer/owner), who decides whether to make such access available to a trusted partner in order to benefit from optimal, secure support. ‘techadmin’ enjoys the same rights as ‘admin’, apart from the right to see or change the ‘admin’ and ‘techadmin’ router access password.

Router remote management in order to configure the WLAN, for example

It is now possible for ‘techadmin’ to carry out various configurations on the Centro Business 2.0 remotely via https:// encryption.

Important

Admin’ must initially create the ‘techadmin’ role with a password in the router portal.
Both ‘admin’ (locally) and ‘superadmin’ (remotely via the Customer Center) can activate temporary ‘techadmin’ remote access by setting the access time (15, 30, 60 mins).
Only one user role can remotely access the router portal at a time.
Permanent remote access has been abolished for security reasons

Procedure for ‘techadmin’ to activate remote access:

1. Activate remote access via the Customer Center and access the router portal with the ‘superadmin’ login
2. Under the menu item ‘Router’, select and save the access time. The ‘superadmin’ session will then be ended.
3. To log in as ‘techadmin’, the existing URL in the browser must be manually changed to https://“WAN-IP“.
4. The login window will be displayed if you type ‘Enter’. Log in with ‘techadmin’ and the password previously set by ‘admin

NAT tables (LAN & DMZ) under Diagnostics (only visible to ‘superadmin’ and ‘techadmin’)

The NAT tables for LAN and DMZ can now be viewed and exported in the router portal under the menu item ‘Diagnostics’. You can therefore identify an active session via the relevant IPs and ports in order to analyse or debug your network.

Bug fixes

- The problem that used to appear in the interim version 9.01.02 – calls interrupting after 15-30 minutes, using HD-Phone Sarnen and Yealink T45G – has been solved.
- The problem with people listening in to calls through handsets connected via DECT and internal call forwarding has been resolved
- Various limitations in the use of IPv6 have been removed
- SBcon telephony connection failures have been corrected
- Centro Business 2.0 configured with IP Passthrough can correctly connect to the Internet after a DSL signal interruption
- Centro Business 2.0 with IP Passthrough without active host configuration, works correctly
- Improved PPP connection with fiber connections
- DNS malfunction related to Internet Backup function has been corrected
- Various improvements to BNS Service stability

Known errors with firmware 9.01.04

- The automatic channel selection of the 5gHz band does not work correctly. With the firmware 9.01.04, the Centro Business 2.0 always selects channel 36. If the WLAN connection quality is disturbed by many other WLAN signals and generates problems with the Internet connection, it is recommended to manually manipulate the channel in the router portal.
- Concerning only firmware intermediate version 9.01.02: In the router-portal, if you click "Check for Update" (under "Router-> Firmware), although the router finds the new firmware version, it cannot be installed. The message "Firmware is up to date" is erroneously displayed. Alternatively, the firmware can be selected and installed locally as a file. The file can be downloaded from the help page.