# Anciennes versions du micrologiciel Centro Business 2.0

Centro Business 2.0
Konfigurationsanleitung

Swisscom (Schweiz) AG
KMU
3050 Bern

swisscom

Release note actuelle

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

Comme nous l'avions annoncé, nous avons reçu un firmware plus récent qui résout également les problèmes ISDN (écho et voix faible). Le déploiement actuel du firmware se poursuit avec la version 9.50.08.

### Erreurs corrigées

- Lorsque tu utilises des téléphones ISDN, tu peux entendre l'autre partie très silencieusement.

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

Important : Dans le firmware 9.50.06 il y a encore une erreur connue lors de l'utilisation de la téléphonie ISDN (présence d'écho ou station distante très silencieuse). Par conséquent, ce micrologiciel n'est actuellement pas utilisé pour les clients InOne PME qui utilisent la VoIP et éventuellement l'ISDN (pas de mise à jour automatique du firmware).

### Erreurs corrigées

- Avec certains téléphones ISDN (notamment le Gigaset), un écho est présent lorsque vous appelez votre correspondant.
- Les clients de Sbcon qui ont des téléphones analogiques connectés à l'interface ATA ne voient pas l'affichage du numéro d'appel et les appels manqués. (CLIP défectueux)
- Les clients qui utilisent PPP Passthrough ont parfois des restrictions de service avec : VPN, configuration des connexions de téléphonie d'entreprise, touches BLF. (Négociation de la taille du MTU)
- Pour les clients utilisant la fonctionnalité PPP Passthrough, une réinitialisation du réseau étendu dans le portail du routeur entraîne une panne du routeur (une réinitialisation matérielle est nécessaire).
- Pour les clients avec l'option MAO BNS & VoIP, le téléphone ne sonne pas sur le groupe de recherche avec sonnerie parallèle et le "BLF" ne fonctionne pas (seule la "Busy Lamp Field List" est visible).
- Les clients disposant de BNS et avec la DMZ connaissent des interruptions occasionnelles qui peuvent être résolues temporairement par un redémarrage du routeur.

## Routeur firmware béta 9.50.04 / B 14+  (Avril, 2021)

### Erreurs corrigées

#### Conflit VLAN10 avec Enterprise Connect (fibre)

Si un client "Enterprise Connect S" configure un VLAN10 sur le port LAN d'une connexion fibre (FTTH & XGS-PON), aucune connexion Internet ne peut être établie (conflit sur le port WAN et LAN avec le même VLAN10). Les installations BNS existantes sont néanmoins affectées si elles configurent ultérieurement un VLAN10 (Access) dans le LAN.

## Routeur firmware béta 9.50.02 / B 14  (Avril, 2021)

### Nouvelles fonctions

#### Désactiver le port Ethernet individuellement

Ethernet Port können neu im Router-Portal unter "Netzwerk" einzeln komplett deaktiviert werden. So können missbräuchliche Geräteverbindungen im LAN unterdrückt werden. Wird an einem deaktivierten Port ein Gerät angeschlossen, leuchtet das LED am Ethernet-Port nicht. Beachten Sie, dass Swisscom im Supportfall nicht weiss, ob Sie diese Funktion nutzten und deshalb allfällige Verbindungsprobleme melden.

## Surveillance dans le portail du routeur pour l'analyse des SPAM

Si un client est identifié dans le réseau Swisscom par un trafic potentiel de SPAM, il est dirigé vers un processus de bac à sable et bloqué en cas de non-respect récurrent. Nous offrons désormais la possibilité d'analyser le trafic via le port 25 et de déterminer quel appareil le déclenche dans le portail du routeur sous "Analysis" → "Connection Monitoring". Cette fonction est uniquement disponible si vous vous connectez en tant que Superadmin ou Techadmin.

## Sécurité améliorée pour le VPN site à site avec le profil IKEv2 (SHA2-256 & PFS)

La nouvelle version du firmware, supporte également la fonction de hachage SHA2-256 avec l'option IKEv2. En outre, il est possible de définir dans les paramètres VPN Peer to Peer (profil IKEv2) si tu veux travailler avec ou sans l'option PFS (Perfect Forward Secrecy). Vers le document d'aide.

## VPN DH Groupes

Plusieurs groupes DH sont pris en charge par le VPN.

## Logs VPN dans l'interface de routeur

Nouveau, vous pouvez également consulter les journaux VPN dans l'interface de routeur, vous pouvez les trouver sous Diagnostic -> System Log .

## Prise en charge de la nouvelle clé USB E3372h-320

Le microprogramme prend également en charge le nouveau Sitick USB 4G pour la sauvegarde sur Internet.

## Fournisseurs DynDNS définis par l' utilisateur possibles Désormais

Il est maintenant possible de faire un enregistrement DynDNS individuel sur le portail du routeur. Nous offrons ainsi une flexibilité élevée vis-à-vis de l'utilisateur. Mais comme de nombreux fournisseurs demandent des configurations très individuelles, il s'agit d'une fonction d'expert, Swisscom offre ni aide ni soutien, ni assistance !

Vous trouverez des conseils et des astuces dans le document d'aide.

## ICMP Redirect

Vous pouvez désactiver l'ICP Redirect sur les itinéraires statiques

## Nouvelles exigences plus strictes concernant le mot de passe du routeur (admin)

Afin de garantir activement la sécurité des installations de nos clients, nous avons décidé de renforcer les exigences relatives au mot de passe pour la connexion au routeur. Au moins 10 caractères et au moins 1 caractère pour chacun des types de caractères suivants:

- Lettres minuscules: Toutes les lettres minuscules; (a...z)
- Lettres majuscules: Toutes les lettres majuscules; (A...Z)
- Chiffres: Tous les chiffres; (0 à 9)
- Caractères spéciaux: Tous les caractères spéciaux courants; @ = + -" * / \ ( ) [ ] { } # % & ? ! € . : , ; $ _(soulignement/underscore)
  sauf < > et espaces € £ § ° ö é Ö Ä à ä ç ~ ¿ ¡

## Erreurs corrigées et connues

corrigé = ✓ connu = ✘

| | Connu depuis la version firmware |
|---|---|
| ✓ Avec certains téléphones ISDN (notamment le Gigaset), un écho est présent lorsque vous appelez votre correspondant. | 9.50.02 |
| ✓ Les clients de Sbcon ne voient pas l'affichage du numéro d'appel et les appels manqués sur l'interface téléphonique analogique (ATA). (CLIP incorrect) | 9.50.02 |
| ✓ Les clients qui utilisent PPP Passthrough ont parfois des restrictions de service avec : VPN, configuration des connexions de téléphonie d'entreprise, touches BLF. (Négociation de la taille du MTU) | 9.50.02 |
| ✓ Pour les clients utilisant la fonctionnalité PPP Passthrough, une réinitialisation du réseau étendu dans le portail du routeur entraîne une panne du routeur (une réinitialisation matérielle est nécessaire). | 9.50.02 |
| ✓ Pour les clients avec l'option MAO BNS & VoIP, le téléphone ne sonne pas sur le groupe de recherche avec sonnerie parallèle et le "BLF" ne fonctionne pas (seule la "Busy Lamp Field List" est visible). | 9.50.02 |
| ✓ Les clients disposant de BNS et avec la DMZ connaissent des interruptions occasionnelles qui peuvent être résolues temporairement par un redémarrage du routeur. | 9.50.02 |
| ✓ Avec certains téléphones RNIS (notamment Gigaset), un écho se produit lorsque l'autre partie est au téléphone. | 9.50.02 |
| ✓ Lorsque tu utilises des téléphones ISDN, tu peux entendre l'autre partie très silencieusement. | 9.50.06 |

**Limitation connue**

| | |
|---|---|
| La restauration de la configuration de Centro Business 2.0 (Backup & Restore), qui a été générée sur une ancienne version de firmware, n'est pas possible en raison du modèle de données fondamentalement révisé. Il est recommandé de créer un fichier de sauvegarde de façon récurrente sur une installation avec un nouveau firmware. Pour plus d'informations sur la création d'une sauvegarde, reportez-vous au document d'aide. | 9.03.xx |


# Router Firmware 9.04.10 / B 13+++ (Janvier 2020)

## Nouvelles fonctionnalités

### Technologie de fibre optique XGS-PON.

Le nouveau firmware permet d'utiliser le Centro Business 2.0 pour la technologie XGS-PON avec un nouveau module SFP (mars 2020).

Le client à besoin d'un nouveau module SFP de Swisscom. Cela permet d'atteindre une vitesse de navigation de max. 1Gbps.

## Erreurs corrigées et connues

corrigé = ✓ connu = ✗

| | Connu depuis la version firmware |
|---|---|
| ✗ PPP Passthrough compatible MTU de 1492 au lieu de 1500 | 8.06.08 |
| ✗ Diverses erreurs de traduction linguistique dans l'interface graphique | 9.01.02 |
| ✗ Le transfert de port est supprimé après une réinitialisation WAN | 8.06.08 |
| ✗ Certains trafics de la DMZ vers le LAN ne sont pas bloqués | 9.02.12 |
| ✗ La restauration sélective ne fonctionne pas correctement | 8.06.08 |
| ✓ Les connexions LAN à la DMZ seront effectuées avec le LAN IP au lieu du routeur WAN IP (ID 3403) | 9.03.xx |

6

Avec le nouveau firmware, le pilote DECT est mis à jour et retarde la disponibilité des services jusqu'à 20 minutes.

**Limitation connue**

La restauration de la configuration de Centro Business 2.0 (Backup & Restore), qui a été générée sur une ancienne version de firmware, n'est pas possible en raison du modèle de données fondamentalement révisé. Il est recommandé de créer un fichier de sauvegarde de façon récurrente sur une installation avec un nouveau firmware. Pour plus d'informations sur la création d'une sauvegarde, reportez-vous au document d'aide.

9.03.xx

## Routeur Firmware 9.04.06 / B13++'(novembre 2019)

### Dépannage

- Le routing  incorrect de la DMZ a été corrigé
- Correction du problème "no audio-pas de son-pas de tonalité" avec les appels SIP
- Correction du problème "no audio-pas de son via DECT
- Amélioration de la manipulation multicast

## Router Firmware 9.04.04 / B 13+ (août 2019)

### Erreurs corrigées

- Problèmes de connexion Internet sporadiques après la mise à jour du micrologiciel sur les connecteurs en cuivre
- Terminaisons sporadiques d'appels téléphoniques en cours (changement de port)
- Optimisation de la configuration de la connexion téléphonique (gestion des codecs)

## Routeur firmware 9.04.02/ B 13  (Juillet, 2019)

### Nouvelles fonctions

#### Prise en charge du "Toolkit for Business" pour le service "Business Internet Services wireless"

Avec le nouveau firmware, le routeur Centro Business 2.0 supporte le "Toolkit for Business" pour le Business Internet Services wireless". Ce service augmente la mobilité de votre accès Internet et permet aux clients professionnels de garantir une meilleure bande passante, même dans les zones peu développées. (via le réseau mobile)

#### Prise en charge du "Toolkit for Business" en tant que protection contre les pannes d'Internet

Avec le nouveau firmware, le routeur Centro Business 2.0 prend en charge non seulement le dongle USB existant, mais aussi le "Toolkit for Business" comme protection contre les pannes (4G).

#### Support du répéteur DECT Gigaset HX

Avec le nouveau firmware, Centro Business 2.0 supporte l'utilisation du futur répéteur DECT Gigaset HX. Le nouveau firmware supporte jusqu'à deux répéteurs et un maximum de 2 téléphones HD peuvent être connectés.

#### Modernisation du cryptage VPN

Les connexions VPN site to site possibles ont été révisées et offrent une sécurité accrue en supportant la méthodologie de cryptage IKEv2.  (Jusqu'à présent IKEv1)

#### Amélioration de la liste des périphériques dans le portail du routeur

L'aperçu de la liste des périphériques dans le portail du routeur offre désormais des informations détaillées sur le réseau. Le port Ethernet (1-4) ou WLAN (2.4/5.0) via lequel le périphérique LAN est connecté est déclaré pour chaque périphérique LAN connecté. La vitesse à laquelle le périphérique fonctionne actuellement avec le Centro Business 2.0 (LAN) est également affichée. Ethernet affiche 10/100/1000Mb, WLAN affiche la vitesse actuelle de la liaison descendante et montante. Pour mettre à jour les informations, la page doit être rechargée.

#### Identifier les conflits IP dans le portail du routeur

Le Centro Business 2.0 signale maintenant un conflit d'adresse IP si des doublons d'adresse IP sont détectés sur le réseau. Un avertissement rouge apparaît sur la page d'aperçu et les entrées concernées sont affichées en rouge dans la liste des appareils. Si un conflit IP est détecté, veuillez contacter votre administrateur réseau.



#### Exécuter la mise à jour locale du firmware la nuit

Afin de ne pas interrompre l'accès Internet d'une entreprise pendant les heures de bureau pour une mise à jour manuelle du firmware, le portail du routeur offre la possibilité d'effectuer

## Adaptations légales de la fonction

⇨ Information complémentaires

### Le WLAN non crypté est bloqué

Avec les modifications de la législation de l'Office fédéral de surveillance, Swisscom doit veiller à ce que des personnes non autorisées ne puissent pas utiliser le WLAN de nos clients de manière abusive. Le WLAN ne peut plus être diffusé de manière non cryptée sur le Centro Business 2.0.

### Exigences plus strictes en matière de mot de passe WLAN WPA2

Les exigences suivantes s'appliquent désormais à la définition d'un mot de passe WLAN :
Le mot de passe doit comporter au moins 10 caractères (16 caractères ou plus sont recommandés) et contenir au moins 1 caractère chacun parmi les types de caractères suivants :

- Lettres minuscules: Toutes les lettres minuscules; (a...z)
- Lettres majuscules: Toutes les lettres majuscules; (A...Z)
- Chiffres: Tous les chiffres; (0 à 9)
- Caractères spéciaux: Tous les caractères spéciaux courants; @ = + -" * / \ ( ) [ ] { } # % & ? ! € . : , ; $ sauf; < > et vierges

Le caractère _(soulignement/underscore) est également autorisé, mais n'est affecté à aucun des types de caractères mentionnés.

Les mots de passe "plus faibles" existants peuvent toujours être utilisés malgré les mises à jour du firmware, mais ils doivent répondre aux exigences lors de la prochaine modification du portail du routeur. Nous vous recommandons de le faire de manière proactive.

### Le "WLAN invité" a été renommé en "WLAN séparé"

Nous appelons maintenant le WLAN invité "WLAN séparé". Avec les modifications de la législation de l'Office fédéral de surveillance, Swisscom doit veiller à ce que des personnes non autorisées ne puissent pas utiliser le WLAN de nos clients de manière abusive. Swisscom recommande à tous les clients PME de ne plus transmettre leurs signaux WLAN ou leurs mots de passe à des inconnus.
Vous trouverez des informations détaillées sur l'adaptation de la loi dans la brochure WLAN du "Service Surveillance de la correspondance par poste et télécommunication".

## Microgiciel 9.02.14 (octobre 2018)

### Nouvelles fonctions

- Aucun

### Corrections des erreurs:

- Le rare problème de synchronisation avec le réseau Swisscom du Centro Business 2.0 avec réglage d'usine (mise en service ou après réinitialisation) est résolu avec ce firmware. En cas de problèmes de synchronisation avec le firmware 9.02.12, le routeur peut être mis à jour manuellement via un appareil local (PC). Vous trouverez ici comment effectuer une mise à jour manuelle (Variante 2 " Actualisation du firmware via la page d'aide").

### Erreurs connues avec le micrologiciel 9.02.14:

- Aucun

## Microgiciel 9.02.12 (juin 2018)

Le firmware est avant tout une version améliorée du firmware 9.02.06 / 9.02.10 et stabilise les installations en utilisant FixIP, port forwarding ou DMZ. Tous les Centro Business 2.0 qui n'utilisent pas encore le firmware 9.02.06 ou FixIP, port forwarding ou DMZ seront automatiquement mis à jour avec la nouvelle version (9.02.12) dans les prochaines semaines. Cependant, vous pouvez mettre à jour manuellement le firmware à partir de la page d'aide officielle de Centro Business 2.0.

### Corrections des erreurs:

- Transfert du port: Si la redirection du port est utilisée sur le Centro Business 2.0 avec FixIP, la redirection du port fonctionne à nouveau correctement après la mise à jour du firmware et après un redémarrage du routeur.
- DynDNS : Le service DynDNS fonctionne à nouveau correctement après la mise à jour du firmware et après un redémarrage du routeur.

### Erreurs connues avec le micrologiciel 9.02.12:

- Dans de rares cas, un routeur avec des réglages d'usine (mise en service ou après réinitialisation) qui souhaite se connecter à Internet via la technologie cuivre ne peut pas se synchroniser avec le réseau Swisscom. Veuillez contacter la hotline SME.

## Microgiciel 9.02.10 (juin 2018)

Le firmware en question est principalement une version améliorée du firmware 9.02.06 et stabilise les installations utilisant FixIP et DMZ. Tous les Centro Business 2.0 qui n'utilisent pas encore le firmware 9.02.06 et qui utilisent FixIP et DMZ seront automatiquement mis à jour vers la nouvelle version (9.02.10) dans les prochaines semaines. Cependant, vous pouvez mettre à jour manuellement le firmware à partir de la page d'aide officielle de Centro Business 2.0.

### Corrections des erreurs:

- DMZ : Le fait que la téléphonie business a des problèmes d'enregistrement ou de connexion dans le cas d'application "DMZ on Port 1" après une interruption ou un redémarrage du PPP a été résolu.
- DMZ : L'erreur qui faisait que la fonction DMZ ne démarrait qu'occasionnellement après une mise à jour du firmware a été corrigée.
- D'autres améliorations de stabilité

### Erreurs connues avec le micrologiciel 9.02.10:

- DynDNS : Le service DynDNS peut occasionnellement être interrompu. Comme solution de contournement, l'option DynDNS peut être désactivée et réactivée dans l'interface graphique du routeur.
- Port forwarding: Si le transfert de port est utilisé sur le Centro Business 2.0 avec FixIP, les règles sont visibles dans le portail du routeur mais ne fonctionnent pas après la mise à jour du firmware de même lors d'un redémarrage du routeur. L'erreur peut être corrigée en désactivant et en réactivant le transfert de port dans le portail du routeur. En évitant un redémarrage du routeur, vous pouvez éviter que l'erreur se reproduise.

## Microgiciel 9.02.06 (mai 2018)

### Nouvelles fonctions

#### Compatibilité avec G.fast

G.fast est une toute nouvelle technologie qui permet d'augmenter considérablement les débits pour la transmission des données sur le réseau fixe cuivre. L'extension continue du réseau vient seulement de commencer. Vérifier la bande passante disponible

#### Compatibilité avec Premium Call

Valable uniquement pour PME Office et inOne PME Office

Il est possible de passer six appels simultanément si l'abonnement comprend au moins six canaux. Désormais les 2 canaux vocaux ISDN peuvent être désactivés, la station de base DECT peut être donc disponible. Le nombre d'appels simultanés est limité comme suit. Les réglages peuvent être faits sur le portail du routeur sous le menu VoIP/Basic Settings. Tout changement de paramètre entraîne un redémarrage du routeur.

| Appels simultanés par technologie | Nombre de canaux tél. avec téléphones ISDN | Nombre de canaux tél. après désactivation ISDN |
|---|---|---|
| Téléphonie analogique (tél.) | 2 | 2 |
| Téléphonie ISDN (ISDN) | 2 | 0 |
| DECT CAT-iq | 2 (HD) Voice | 2 (HD Voice) + 2 (Voice) |

#### Configuration manuelle du serveur DNS

Dans le portail du routeur, le mode DNS manuel peut maintenant être activé sous l'option de menu "Paramètres de base Internet", permettant de définir ainsi un serveur DNS principal préféré ainsi qu'un deuxième serveur. Cette fonction permet de contourner l`Internet Guard récemment introduit.

#### Nouveau rôle utilisateur «techadmin» pour un service à la clientèle optimal de la part du partenaire informatique

Le rôle «techadmin» a été créé en plus des rôles utilisateurs «admin» pour l'accès local au portail du routeur et «superadmin» pour l'accès à distance temporaire (activation dans l'espace clients).

Une fois activé, ce rôle permet d'accéder temporairement au portail du routeur aussi bien via le LAN local que via l'accès à distance (https:// uniquement). Le mot de passe fixe et à définir ne peut être créé initialement que par l'«admin» (client/titulaire). Il décide s'il souhaite mettre cet accès à disposition de son partenaire de confiance et bénéficier ainsi d'une prise en charge sûre et optimale. Le «techadmin» dispose des mêmes droits que l'admin, mais il ne peut ni consulter ni modifier le mot de passe d'accès au routeur pour «admin» et «techadmin».

## Gestion à distance du routeur pour configurer le WLAN par exemple

Désormais, il est possible de procéder à divers paramétrages sur le routeur Centro Business 2.0 en tant que «techadmin» via l'accès à distance https:// (remote).

Documentation de support détaillée

**Remarques importantes:**

- L'«admin» doit tout d'abord définir le «techadmin» avec un mot de passe sur le portail du routeur.
- L'«admin» local et le «superadmin» à distance (via l'espace clients) peuvent activer l'accès à distance temporaire «techadmin» en définissant la durée de l'accès (15, 30 ou 60 minutes).
- Un seul rôle utilisateur à distance à la fois peut accéder au portail du routeur
- Pour des raisons de sécurité, les possibilités d'accès à distance systématique ont été supprimées.

Procédure pour le «techadmin» qui souhaite activer l'accès à distance

1. Activer l'accès à distance via l'espace clients et accéder au portail du routeur avec l'accès «superadmin».
2. Sélectionner et sauvegarder la durée de connexion sous le menu «Routeur». La session «superadmin» est ainsi bloquée.
3. Pour vous connecter en tant que «techadmin», l'URL existante doit être modifiée manuellement dans le navigateur avec https://"WAN-IP".
4. La fenêtre de login s'affiche en appuyant sur la touche «Enter». Connexion avec «techadmin» et le mot de passe prédéfini par l'«admin».

## Diagnostic tables NAT (LAN et DMZ) (visible exclusivement pour le «superadmin» et le «techadmin»)

Désormais, les tables NAT pour LAN et DMZ peuvent être consultées et exportées sur le portail du routeur, sous le menu Diagnostic. Vous pouvez ainsi identifier une session active via l'adresse IP et le port respectifs, et l'utiliser pour l'analyse et le dépannage de votre réseau.

Vous trouverez ici plus d'informations sur le fonctionnement NAT.

## Corrections des erreurs pour les mises à niveau à partir du 8.06.08:

- Le problème avec la conférence à quatre involontaire, les combinés raccordés par DECT et la redirection interne des appels a été résolu.
- Plusieurs restrictions ont été levées pour l'utilisation de IPv6.
- Les interruptions de communication pour la téléphonie SBcon ont été corrigées.
- Les routeurs Centro Business 2.0 configurés par IP-Passthrough se reconnectent correctement à Internet après une interruption du signal DSL.
- La configuration IP Passthrough avec Centro Business 2.0 sans active Host, fonctionne correctement
- Meilleur comportement de l'établissement de la communication PPP pour les raccordements fibre optique.
- Diverses améliorations concernant la stabilité du service BNS.
- Le comportement incorrect du DNS par rapport à la fonction Internet-Backup a pu être corrigé.

Recommandation importante:

Les clients qui ont désactivé dans le passé l'Internet Backup Stick en raison de limitations de service, doivent les reconnecter au Centro Business 2.0 afin de bénéficier de la disponibilité du service sur le réseau mobile en cas de panne.

## Corrections des erreurs pour les mises à niveau à partir du 9.01.04:

- Pour des raisons de sécurité, les appels avec SIP Credentials locales sur le réseau sans fil invité ne sont plus pris en charge.
- Pour les connexions avec une adresse IP fixe, les paramètres de Portforwarding sont correctement repris après une WAN Reset.
- Les connexions de la conférence internes et externes fonctionnent maintenant correctement.
- Plusieurs problèmes de connexion et interruptions (après environ 15 minutes) dans la téléphonie, ainsi que des problèmes avec l'affichage BLF ont été corrigés.
- Diverses améliorations dans la configuration des connexions via fibre optique et DSL, ainsi que des améliorations de la stabilité DHCP dans le réseau local.
- La sélection automatique du canal de la bande 5gHz fonctionne à nouveau correctement.
- La DMZ fonctionne de nouveau correctement après une interruption de la connexion PPP.

## Corrections des erreurs pour les mises à niveau à partir du 9.02.04:

- L'abonné B peut confirmer correctement les appels à l'aide de la numérotation par clavier (DTMF).

## Erreurs connues avec le micrologiciel 9.02.06:

- DMZ: la fonction DMZ ne fonctionne pas après une mise à niveau FW. L'erreur peut être corrigée avec un désactivation et réactivation dans le portail du routeur.
- DynDNS: il peut arriver que le service DynDNS soit occasionnellement interrompu. Comme Workaround, l'option DynDNS peut être désactivée et réactivée dans le Router GUI.
- Lors d'une interruption de session PPP, il arrive parfois que dans le cas de "DMZ sur Port 1", la relative téléphonie Business (PBX@HET et SIP Phones avec Smart Business Connect et inOne PME) ait des problèmes avec l'enregistrement ou la téléphonie. Ce problème est également présent sur les versions antérieures du firmware et peut être corrigé en redémarrant le routeur.
- Concerne uniquement la version intermédiaire du Firmware 9.01.04:
- Si on clique, via le portail du routeur (192.168.1.1), sur le bouton de mise à jour "Rechercher mise à jour" sous "Routeur" -> "Logiciel" le routeur trouve la nouvelle version de Firmware 9.02.06, mais celle-ci ne peut pas être installée. Le message suivant est envoyé par erreur: Logiciel est à jour. Alternativement, le Firmware peut être sélectionné et installé localement en tant que fichier.

## Microgiciel 9.02.04 (Mars 2018)

### Nouvelles fonctions

#### Compatibilité avec G.fast

G.fast est une toute nouvelle technologie qui permet d'augmenter considérablement les débits pour la transmission des données sur le réseau fixe cuivre. L'extension continue du réseau vient seulement de commencer. Vérifier la bande passante disponible

#### Compatibilité avec Premium Call

Valable uniquement pour PME Office et inOne PME Office

Il est possible de passer six appels simultanément si l'abonnement comprend au moins six canaux. Désormais les 2 canaux vocaux ISDN peuvent être désactivés, la station de base DECT peut être donc disponible. Le nombre d'appels simultanés est limité comme suit. Les réglages peuvent être faits sur le portail du routeur sous le menu VoIP/Basic Settings. Tout changement de paramètre entraîne un redémarrage du routeur.

| Appels simultanés par technologie | Nombre de canaux tél. avec téléphones ISDN | Nombre de canaux tél. après désactivation ISDN |
|---|---|---|
| Téléphonie analogique (tél.) | 2 | 2 |
| Téléphonie ISDN (ISDN) | 2 | 0 |
| DECT CAT-iq | 2 (HD) Voice | 2 (HD Voice) + 2 (Voice) |

#### Nouveau rôle utilisateur «techadmin» pour un service à la clientèle optimal de la part du partenaire informatique

Le rôle «techadmin» a été créé en plus des rôles utilisateurs «admin» pour l'accès local au portail du routeur et «superadmin» pour l'accès à distance temporaire (activation dans l'espace clients).

Une fois activé, ce rôle permet d'accéder temporairement au portail du routeur aussi bien via le LAN local que via l'accès à distance (https:// uniquement). Le mot de passe fixe et à définir ne peut être créé initialement que par l'«admin» (client/titulaire). Il décide s'il souhaite mettre cet accès à disposition de son partenaire de confiance et bénéficier ainsi d'une prise en charge sûre et optimale. Le «techadmin» dispose des mêmes droits que l'admin, mais il ne peut ni consulter ni modifier le mot de passe d'accès au routeur pour «admin» et «techadmin».

## Gestion à distance du routeur pour configurer le WLAN par exemple

Désormais, il est possible de procéder à divers paramétrages sur le routeur Centro Business 2.0 en tant que «techadmin» via l'accès à distance https:// (remote).

Documentation de support détaillée

Remarques importantes:

- L'«admin» doit tout d'abord définir le «techadmin» avec un mot de passe sur le portail du routeur.
- L'«admin» local et le «superadmin» à distance (via l'espace clients) peuvent activer l'accès à distance temporaire «techadmin» en définissant la durée de l'accès (15, 30 ou 60 minutes).
- Un seul rôle utilisateur à distance à la fois peut accéder au portail du routeur
- Pour des raisons de sécurité, les possibilités d'accès à distance systématique ont été supprimées.

Procédure pour le «techadmin» qui souhaite activer l'accès à distance

1. Activer l'accès à distance via l'espace clients et accéder au portail du routeur avec l'accès «superadmin».
2. Sélectionner et sauvegarder la durée de connexion sous le menu «Routeur». La session «superadmin» est ainsi bloquée.
3. Pour vous connecter en tant que «techadmin», l'URL existante doit être modifiée manuellement dans le navigateur avec https://"WAN-IP".
4. La fenêtre de login s'affiche en appuyant sur la touche «Enter». Connexion avec «techadmin» et le mot de passe prédéfini par l'«admin».

## Diagnostic tables NAT (LAN et DMZ) (visible exclusivement pour le «superadmin» et le «techadmin»)

Désormais, les tables NAT pour LAN et DMZ peuvent être consultées et exportées sur le portail du routeur, sous le menu Diagnostic. Vous pouvez ainsi identifier une session active via l'adresse IP et le port respectifs, et l'utiliser pour l'analyse et le dépannage de votre réseau.

## Corrections

- Pour des raisons de sécurité, les appels avec SIP Credentials locales sur le réseau sans fil invité ne sont plus pris en charge.
- Pour les connexions avec une adresse IP fixe, les paramètres de Portforwarding sont correctement repris après une WAN Reset.
- Les connexions de la conférence internes et externes fonctionnent maintenant correctement.
- Plusieurs problèmes de connexion et interruptions (après environ 15 minutes) dans la téléphonie, ainsi que des problèmes avec l'affichage BLF ont été corrigés.
- Diverses améliorations dans la configuration des connexions via fibre optique et DSL, ainsi que des améliorations de la stabilité DHCP dans le réseau local.
- La sélection automatique du canal de la bande 5gHz fonctionne à nouveau correctement.
- La DMZ fonctionne de nouveau correctement après une interruption de la connexion PPP.

## Erreurs connues avec le micrologiciel 9.02.04

- Update Button: En raison d'une mauvaise version du micrologiciel, la mise à jour de celui-ci via le bouton "mise à jour" ne fonctionne pas correctement. En guise d'alternative, le micrologiciel peut être téléchargé puis installé manuellement sur le routeur via l'interface de ce dernier.
- DynDNS: il peut arriver que le service DynDNS soit occasionnellement interrompu. Comme Workaround, l'option DynDNS peut être désactivée et réactivée dans le Router GUI.
- DMZ: la fonction DMZ ne fonctionne pas après une mise à niveau FW. L'erreur peut être corrigée avec un désactivation et réactivation dans le portail du routeur.
- DTMF: dans le processus de numérotation multifréquence, l'interlocuteur B ne peut pas confirmer un signal de numérotation avec les touches par l'intermédiaire d'une station de base DECT.

## Microgiciel 9.01.04 (Septembre 2017)

### Nouvelles fonctions:

#### Compatibilité avec G.fast

G.fast est une toute nouvelle technologie qui permet d'augmenter considérablement les débits pour la transmission des données sur le réseau fixe cuivre. L'extension continue du réseau vient seulement de commencer. Vérifier la bande passante disponible

#### Compatibilité avec Premium Call

Valable uniquement pour PME Office et inOne PME Office

Il est possible de passer six appels simultanément si l'abonnement comprend au moins six canaux. Désormais les 2 canaux vocaux ISDN peuvent être désactivés, la station de base DECT peut être donc disponible. Le nombre d'appels simultanés est limité comme suit. Les réglages peuvent être faits sur le portail du routeur sous le menu VoIP/Basic Settings. Tout changement de paramètre entraîne un redémarrage du routeur.

| Appels simultanés par technologie | Nombre de canaux tél. avec téléphones ISDN | Nombre de canaux tél. après désactivation ISDN |
|---|---|---|
| Téléphonie analogique (tél.) | 2 | 2 |
| Téléphonie ISDN (ISDN) | 2 | 0 |
| DECT CAT-iq | 2 (HD) Voice | 2 (HD Voice) + 2 (Voice) |

#### Nouveau rôle utilisateur «techadmin» pour un service à la clientèle optimal de la part du partenaire informatique

Le rôle «techadmin» a été créé en plus des rôles utilisateurs «admin» pour l'accès local au portail du routeur et «superadmin» pour l'accès à distance temporaire (activation dans l'espace clients).

Une fois activé, ce rôle permet d'accéder temporairement au portail du routeur aussi bien via le LAN local que via l'accès à distance (https:// uniquement). Le mot de passe fixe et à définir ne peut être créé initialement que par l'«admin» (client/titulaire). Il décide s'il souhaite mettre cet accès à disposition de son partenaire de confiance et bénéficier ainsi d'une prise en charge sûre et optimale. Le «techadmin» dispose des mêmes droits que l'admin, mais il ne peut ni consulter ni modifier le mot de passe d'accès au routeur pour «admin» et «techadmin».

## Gestion à distance du routeur pour configurer le WLAN par exemple

Désormais, il est possible de procéder à divers paramétrages sur le routeur Centro Business 2.0 en tant que «techadmin» via l'accès à distance https:// (remote).

Documentation de support détaillée

Remarques importantes:

- L'«admin» doit tout d'abord définir le «techadmin» avec un mot de passe sur le portail du routeur.
- L'«admin» local et le «superadmin» à distance (via l'espace clients) peuvent activer l'accès à distance temporaire «techadmin» en définissant la durée de l'accès (15, 30 ou 60 minutes).
- Un seul rôle utilisateur à distance à la fois peut accéder au portail du routeur
- Pour des raisons de sécurité, les possibilités d'accès à distance systématique ont été supprimées.

Procédure pour le «techadmin» qui souhaite activer l'accès à distance

1. Activer l'accès à distance via l'espace clients et accéder au portail du routeur avec l'accès «superadmin».
2. Sélectionner et sauvegarder la durée de connexion sous le menu «Routeur». La session «superadmin» est ainsi bloquée.
3. Pour vous connecter en tant que «techadmin», l'URL existante doit être modifiée manuellement dans le navigateur avec https://"WAN-IP".
4. La fenêtre de login s'affiche en appuyant sur la touche «Enter». Connexion avec «techadmin» et le mot de passe prédéfini par l'«admin».

## Diagnostic tables NAT (LAN et DMZ) (visible exclusivement pour le «superadmin» et le «techadmin»)

Désormais, les tables NAT pour LAN et DMZ peuvent être consultées et exportées sur le portail du routeur, sous le menu Diagnostic. Vous pouvez ainsi identifier une session active via l'adresse IP et le port respectifs, et l'utiliser pour l'analyse et le dépannage de votre réseau.

## Corrections

- Le problème dans la version intermédiaire 9.01.02 pour les appels via HD-Phone Sarnen et Yealink T46G interrompus après 15-30 minutes, a été résolu.
- Le problème avec la conférence à quatre involontaire, les combinés raccordés par DECT et la redirection interne des appels a été résolu.
- Plusieurs restrictions ont été levées pour l'utilisation de IPv6.
- Les interruptions de communication pour la téléphonie SBcon ont été corrigées.
- Les routeurs Centro Business 2.0 configurés par IP-Passthrough se reconnectent correctement à Internet après une interruption du signal DSL.
- La configuration IP Passthrough avec Centro Business 2.0 sans active Host, fonctionne correctement.
- Meilleur comportement de l'établissement de la communication PPP pour les raccordements fibre optique.
- Le problème de comportement DNS en lien avec la fonction Internet Backup a pu être corrigé.
- Diverses améliorations concernant la stabilité du service BNS.

## Erreurs connues avec le micrologiciel 9.01.04

- La sélection automatique du canal dans la bande 5gHz ne fonctionne pas correctement. Le Centro Business 2.0 sélectionne toujours le canal 36 avec le firmware 9.01.04. Si la qualité de la connexion WLAN est perturbée par de nombreux autres signaux WLAN et cause des problèmes de connexion Internet, il est recommandé d'adapter manuellement le canal sur le portail du routeur.
- Concerne uniquement la version intermédiaire du Firmware 9.01.02: Si on clique, via le portail du routeur (192.168.1.1), sur le bouton de mise à jour "Rechercher mise à jour" sous "Routeur" -> "Logiciel" le routeur trouve la nouvelle version de Firmware 9.01.04, mais celle-ci ne peut pas être installée. Le message suivant est envoyé par erreur: Logiciel est à jour. Alternativement, le Firmware peut être sélectionné et installé localement en tant que fichier. Le fichier du Firmware peut être téléchargé à partir de la page d'aide.

## Microgiciel 9.01.04 (Septembre 2017)

### Nouvelles fonctions:

#### Compatibilité avec G.fast

G.fast est une toute nouvelle technologie qui permet d'augmenter considérablement les débits pour la transmission des données sur le réseau fixe cuivre. L'extension continue du réseau vient seulement de commencer. Vérifier la bande passante disponible

#### Compatibilité avec Premium Call

Valable uniquement pour PME Office et inOne PME Office

Il est possible de passer six appels simultanément si l'abonnement comprend au moins six canaux. Désormais les 2 canaux vocaux ISDN peuvent être désactivés, la station de base DECT peut être donc disponible. Le nombre d'appels simultanés est limité comme suit. Les réglages peuvent être faits sur le portail du routeur sous le menu VoIP/Basic Settings. Tout changement de paramètre entraîne un redémarrage du routeur.

| Appels simultanés par technologie | Nombre de canaux tél. avec téléphones ISDN | Nombre de canaux tél. après désactivation ISDN |
|---|---|---|
| Téléphonie analogique (tél.) | 2 | 2 |
| Téléphonie ISDN (ISDN) | 2 | 0 |
| DECT CAT-iq | 2 (HD) Voice | 2 (HD Voice) + 2 (Voice) |

#### Nouveau rôle utilisateur «techadmin» pour un service à la clientèle optimal de la part du partenaire informatique

Le rôle «techadmin» a été créé en plus des rôles utilisateurs «admin» pour l'accès local au portail du routeur et «superadmin» pour l'accès à distance temporaire (activation dans l'espace clients).

Une fois activé, ce rôle permet d'accéder temporairement au portail du routeur aussi bien via le LAN local que via l'accès à distance (https:// uniquement). Le mot de passe fixe et à définir ne peut être créé initialement que par l'«admin» (client/titulaire). Il décide s'il souhaite mettre cet accès à disposition de son partenaire de confiance et bénéficier ainsi d'une prise en charge sûre et optimale. Le «techadmin» dispose des mêmes droits que l'admin, mais il ne peut ni consulter ni modifier le mot de passe d'accès au routeur pour «admin» et «techadmin».