Ältere Firmware Versionen Centro Business 2.0

Centro Business 2.0
Konfigurationsanleitung

Swisscom (Schweiz) AG
KMU
3050 Bern

swisscom

Aktuelle Releasenote

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

Wie angekündigt haben wir nun eine neuere Firmware erhalten, welche auch die ISDN Probleme (Echo & Leise Stimme) löst. Der aktuell laufende Firmware-Rollout wird mit der 9.50.08 Version weitergeführt.

Behobene Fehler

- Bei Verwendung von ISDN Telefonen, ist der Gesprächspartner sehr leise zu hören

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

Info: In der Firmware 9.50.06 gibt es heute noch einen bekannten Fehler bei der Verwendung von ISDN Telefonie (Echo bzw. Gegenstelle sehr leise). Deshalb wird diese Firmware aktuell nicht für InOne KMU Kunden welche VoIP und somit ggfl. ISDN verwenden, eingesetzt. (kein automatisches Firmware-Update).

Behobene Fehler

- Diverse Stabilisierungen für Business Network Solution (BNS & EC-S)
- Im BNS Betrieb leuchtet die WLAN LED am Router fälschlicherweise blau, obschon im Dashboard alle WLAN Signale deaktiviert sind.
- Bei gewissen ISDN Telefonen (vor allem Gigaset) entsteht beim telefonieren ein Echo beim Gesprächspartner
- Sbcon Kunden welche analoge Telefone an der ATA Schnittstelle angeschlossen haben, sehen keine Rufnummer Anzeige und verpasste Anrufe. (CLIP fehlerhaft)
- Kunden welche PPP Passthrough nutzen haben teilweise Serviceeinschränkungen bei: VPN-, Business Telefonie Verbindungsaufbau, BLF-Tasten. (Aushandlung der MTU Size)
- Bei Kunden welche PPP Passthrough nutzen, führt ein WAN Reset im Router-Portal dazu, dass PPP Passthrough deaktiviert wird.
- Bei Kunden mit MAO BNS & VoIP klingelt das Telefon bei Sammelanschluss mit parallel Ringing nicht und die "BLF" funktioniert nicht (lediglich "Besetztlampenfeldliste" sichtbar)
- Kunden mit BNS und DMZ haben vereinzelt Unterbrüche.

Router Firmware 9.50.04 / B14+ (April 2021)

Behobene Fehler

VLAN10 Konflikt bei Enterprise Connect (Glasfaser)

Wenn ein "Enterprise Connect S" Kunde an einem Glasfaser Anschluss (FTTH & XGS-PON) auf dem LAN-Port ein VLAN10 konfiguriert, kann keine Internetverbindung etabliert werden (Konflikt auf WAN und LAN Port mit gleichem VLAN10) Bestehende BNS Installationen sind gleichwohl betroffen wenn diese nachträglich ein VLAN10 (Access) im LAN einrichten

Router Firmware 9.50.02 / B14 (April 2021)

Neue Funktionen

Ethernet-Port einzeln deaktivieren

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.

Monitoring im Router-Portal für SPAM Analyse

Wird ein Kunde im Swisscom-Netz durch potentiellen SPAM-Verkehr identifiziert, wird er in einen Sandbox-Prozess geleitet und bei wiederkehrender Missachtung gesperrt. Neu bieten wir im Router-Portal unter "Analyse" → "Connection Monitoring" die Option an, den Verkehr via Port 25 zu analysieren und zu ermitteln welches Gerät diesen auslöst. Diese Funktion können sie nur nutzen, wenn Sie sich via Superadmin oder Techadmin einloggen.

Verbesserte Sicherheit bei Site-to-Site VPN mit IKEv2 Profil (SHA2-256 & PFS)

Mit der neuen Firmware unterstützen wir mit IKEv2 auch die Hashfunktion SHA2-256. Zudem kann man bei der Peer to Peer VPN Einstellungen (IKEv2 Profile) entscheiden, ob man mit oder ohne PFS Option (Perfect Forward Secrecy) arbeiten möchte. Zum Hilfedokument.

VPN DH Gruppen

Neu werden beim VPN mehrere DH Gruppen unterstützt.

VPN Logs im Router GUI

Neu können Sie im Router GUI auch die VPN Logs ansehen, Sie finden diese unter Diagnostik -> System Log .

Support des neuen USB Stick E3372h-320

Die Firmware unterstütz auch den neue 4G USB Stick für das Internet Backup.

Benutzerdefinierter DynDNS Anbieter/Provider möglich

Neu erlauben wir im Router-Portal einen individuellen DynDNS Eintrag vorzunehmen. So bieten wir hohe Flexibilität gegenüber dem Anwender. Da aber die vielen Anbieter sehr individuelle Konfigurationen verlangen, gilt: Dies ist eine Experten-Funktion, Swisscom bietet weder Hilfe noch unterstützen wir mit Support! Tipps und Tricks finden Sie im Hilfe-Dokument

ICMP Redirect

Neu können Sie bei statischen routen das ICP Redirect ausschalten

Neu gelten verschärfte Router-Passwort (Admin) Anforderungen

Um die Sicherheit unserer Kunden–Installationen aktiv zu gewährleisten haben wir entschieden die Passwortanforderungen für das Router-Login zu verschärfen: Mindestens 10 Characters und aus folgenden Zeichen-Typen je mindestens 1 Zeichen enthalten:

- Kleinbuchstaben: Alle Kleinbuchstaben; also a...z
- Grossbuchstaben: Alle Grossbuchstaben; also A...Z
- Zahlen: Alle Zahlen; von 0 bis 9
- Sonderzeichen: Alle gängigen Sonderzeichen; @ = + -" * / \ ( ) [ ] { } # % & ? ! € . : , ; $ _(Unterstrich/Underscore)
  ausser; < > und Leerzeichen€ £ § ° ö é Ö Ä à ä ç ~ ¿ ¡

Bestehende "schwächere" Passwörter können zwar trotz Firmware-Aktualisierung weiterverwendet werden, müssen aber die Anforderungen mit der nächster Änderung im Router-Portal erfüllen. Wir empfehlen Ihnen, dies proaktiv zu machen.

Fehlerbehebungen und Verbesserungen

behoben = ✓ bekannt = X	bekannt seit Firmware-Version
✓ Sbcon Kunde sehen an der analogen Telefon Schnittstelle (ATA) keine Rufnummer Anzeige und verpasste Anrufe. (CLIP fehlerhaft)	9.50.02
✓ Kunden welche PPP Passthrough nutzen haben teilweise Serviceeinschränkungen bei: VPN-, Business Telefonie Verbindungsaufbau, BLF-Tasten. (Aushandlung der MTU Size)	9.50.02
✓ Bei Kunden welche PPP Passthrough nutzen, führt ein WAN Reset im Router-Portal dazu, dass PPP Passthrough deaktiviert wird. Die Funktion kann einfach wieder aktiviert werden.	9.50.02
✓ Bei Kunden mit MAO BNS & VoIP klingelt das Telefon bei Sammelanschluss mit parallel Ringing nicht und die "BLF" funktioniert nicht (lediglich "Besetztlampenfeldliste" sichtbar)	9.50.02
✓ Kunden mit BNS und DMZ haben vereinzelt Unterbrüche, welche mit Router-Neustart temporär gelöst werden können	9.50.02
✓ Bei gewissen ISDN Telefonen (vor allem Gigaset) entsteht beim telefonieren ein Echo beim Gesprächspartner	9.50.02
✓ Bei Verwendung von ISDN Telefonen, ist der Gesprächspartner sehr leise zu hören	9.50.06
Bekannte Limitation: Die Wiederherstellung der Centro Business 2.0 Konfiguration (Backup & Restore) welche auf einer älteren Firmware-Version generiert wurde, ist aufgrund des fundamental überarbeiteten Datenmodells nicht möglich. Es empfiehlt sich, auf einer Installation mit neuer Firmware wiederkehrend ein Backup File zu erstellen. Weitere Infos zur Backup Erstellung siehe Hilfedokument.	9.03.xx

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

Neue Funktionen

XGS-PON Glasfasertechnologie.

Die neue Firmware ermöglich es, dass der Centro Business 2.0 auf der kommenden XGS-PON Technologie (März 2020) mit einem neuen SFP Modul weiterverwendet werden kann.

Der Kunde benötigt dazu ein neues SFP Modul von Swisscom. Damit kann eine Surfgeschwindigkeit von Max. 1Gbit/s erreicht werden.

Behobene und bekannte Fehler

behoben = ✓ bekannt = X	bekannt seit Firmware-Version
× PPP Passthrough Modus unterstützt ein MTU von 1492 anstatt 1500 (ID 3012)	8.06.08
× Diverse Sprachübersetzungsfehler im GUI	9.01.02
× Portweiterleitungen werden nach einem WAN reset gelöscht	8.06.08
× Gewisser Traffic von der DMZ ins LAN wird nicht geblockt (ID 4255)	9.02.12
× Selektives Restoring funktioniert nicht richtig (ID 3675)	8.06.08
✓ LAN Verbindungen in die DMZ erfolgen mit der LAN IP anstatt mit der Router-WAN IP (ID 3403)	9.03.xx

Mit der neuen Firmware wird der DECT Treiber aktualisiert und verzögert die Verfügbarkeit der Dienste um bis zu 20 Minuten

Bekannte Limitation:
Die Wiederherstellung der Centro Business 2.0 Konfiguration (Backup & Restore) welche auf einer älteren Firmware-Version generiert wurde, ist aufgrund des fundamental überarbeiteten Datenmodells nicht möglich. Es empfiehlt sich, auf einer Installation mit neuer Firmware wiederkehrend ein Backup File zu erstellen. Weitere Infos zur Backup Erstellung siehe Hilfedokument. — 9.03.xx

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

Fehlerbehebung

- Falsches DMZ Routing wurde behoben
- "No Audio-Teilnehmer hören sich gegenseitig nicht" Problem bei SIP Calls wurde behoben
- "No Audio-Teilnehmer hören sich gegenseitig nicht" Problem via DECT wurde behoben
- Verbesserung im Multicast Handling

Router Firmware 9.04.04 / B 13+ (August 2019)

Fehlerbehebung

- Sporadische Internet Verbindungsprobleme nach Firmwareupdate auf Kupfer-Anschlüssen
- Sporadische Abbrüche von laufenden Telefonaten (Port Change)
- Optimierung des Telefon Verbindungsaufbau (Codec Handling)

Router Firmware 9.04.02 / B 13 (Juli 2019)

Neue Funktionen

Unterstützung des "Toolkit for Business" für "Business Internet Services wireless"

Mit der neuen Firmware unterstützt der Centro Business 2.0 Router das "Toolkit for Business" für "Business Internet Services wireless". Dieser Service steigert die Mobilität Ihres Internetzugangs und ermöglicht Geschäftskunden auch in schwach erschlossenen Gebieten eine verbesserte Bandbreite gewährleisten zu können. (über Mobilenetz)

Unterstützung des "Toolkit for Business" als Internetausfallsicherung

Mit der neuen Firmware unterstützt der Centro Business 2.0 Router neben dem bestehenden USB Dongle auch das "Toolkit for Business" als Ausfallsicherung (4G).

Unterstützung des DECT Gigaset Repeater HX

Mit der neuen Firmware unterstützt die Centro Business 2.0 die Verwendung des künftig angebotenen DECT Gigaset Repeater HX. Die neue Firmware unterstützt bis zu zwei Repeater und es können max. 2 HD-Phones verbunden werden.

Modernisierung der VPN Verschlüsselung

Die möglichen Site to Site VPN Verbindungen wurden überarbeitet und bieten erhöhte Sicherheit durch die Unterstützung der IKEv2 Verschlüsselungsmethodik. (Bis jetzt IKEv1)

Verbesserte Geräteliste im Router-Portal

Neu bietet die Geräteliste-Übersicht im Router-Portal erweiterte Informationen zum Netzwerk. Zu dem jeweiligen verbundenen LAN-Gerät wird deklariert, über welchen Ethernet-Port (1-4) beziehungsweise welches WLAN (2.4/5.0) es verbunden ist. Zudem wird ausgewiesen mit welcher Geschwindigkeit das Gerät mit der Centro Business 2.0 (LAN) aktuell arbeitet. Bei Ethernet wird 10/100/1000Mb, bei WLAN wird die aktuelle Down- und Up-Link Geschwindigkeit angezeigt. Um die Angaben zu aktualisieren, muss die Seite neu geladen werden.

IP-Konflikte im Router-Portal identifizieren

Neu signalisiert der Centro Business 2.0 einen IP-Konflikt, wenn im Netzwerk IP-Adress-Duplikate erkannt wurden. Auf der Übersichtsseite erscheint ein roter Warnhinweis und in der Geräteliste werden die betroffen Einträge rot dargestellt. Bei einem erkannten IP-Konflikt wenden Sie bitte an Ihren Netzwerk-Administrator.

Lokale Firmware-Aktualisierung in der Nacht ausführen lassen

Um den Internet-Zugang eines Unternehmens nicht während der Bürozeiten, für eine manuelle Firmware-Aktualisierung zu unterbrechen, bietet sich im Router-Portal die Option an, das Update erst in der kommenden Nacht (2:00) automatisch durchzuführen. Wie sie die verzögerte Firmware-Aktualisierung durchführen, erfahren sie in dieser Anleitung. Achtung! Bei einem zwischenzeitlichen Firmware-Update, einem Reboot oder einem Reset des Centro Business 2.0 wird die pendente Firmware-Aktualisierung gelöscht.

Kleinere IPv4 Subnetze als /24 in LAN konfigurieren

Um mehr Kontrolle über Netzwerkgrösse zu erlangen, können neu Subnetze zwischen "/8" (16mio IP-Adressen) bis "/30" (2 IP-Adressen) konfiguriert werden. Bis jetzt war die kleinste Option "/24" (254 IP Adressen).

Gesetzliche Funktionsanpassungen

⇨ Weitere Informationen

Unverschlüsseltes WLAN wird gesperrt

Mit den Anpassungen der Gesetzgebungen des Bundesamt für Überwachung, muss die Swisscom sicherstellen, dass Unbefugte nicht das WLAN unserer Kunden missbräuchlich verwenden dürfen. Neu kann das WLAN auf dem Centro Business 2.0 nicht mehr unverschlüsselt ausgestrahlt werden.

Strengere WPA2 WLAN Passwortanforderungen

Neu gelten folgende Anforderungen bei der Festlegung eines WLAN-Passwortes: Das Passwort muss mindestens 10 Zeichen lang sein (Empfohlen sind 16 Zeichen oder mehr) und aus folgenden Zeichen-Typen je mindestens 1 Zeichen enthalten:

– Kleinbuchstaben:	Alle Kleinbuchstaben; also a...z
– Grossbuchstaben:	Alle Grossbuchstaben; also A...Z
– Zahlen:	Alle Zahlen; von 0 bis 9
– Sonderzeichen:	Alle gängigen Sonderzeichen; @ = + - " * / \ ( ) [ ] { } # % & ? ! € . : , ; $ ausser; < > und Leerzeichen

Das Zeichen _(Unterstrich/Underscore) ist ebenfalls erlaubt, wird aber keinem der genannten Zeichen-Typen zugeordnet.

Bestehende "schwächere" Passwörter können zwar trotz Firmware-Aktualisierung weiterverwendet werden, müssen aber die Anforderungen mit der nächster Änderung im Router-Portal erfüllen. Wir empfehlen Ihnen, dies proaktiv zu machen.

U enennung des Gast-WLAN zu "separiertes WLAN"

Neu nennen wir das Gast-WLAN "separiertes WLAN". Mit den Anpassungen der Gesetzgebungen des Bundesamt für Überwachung, muss Swisscom sicherstellen, dass Unbefugte nicht das WLAN unserer Kunden missbräuchlich verwenden können. Swisscom empfiehlt allen KMU Kunden, dass Sie ihre WLAN Signale, bzw. deren Passwörter, nicht mehr an Unbekannte weitergibt. Details zur Gesetzesanpassung findet man im Merkblatt WLAN des "Dienst Überwachung Post- und Fernmeldeverkehr".

Router Firmware 9.02.14 (Oktober 2018)

- Keine

Fehlerbehebungen

- Das seltene Synchronisationsproblem mit dem Swisscom-Netz des Centro Business 2.0 mit Werkseinstellung (Inbetriebnahme oder nach Reset) wird mit dieser Firmware gelöst. Bei Synchronisationsproblemen mit der Firmware 9.02.12 kann der Router manuell über ein lokales Gerät (PC) aktualisiert werden. Wie Sie ein manuelles Update machen, erfahren Sie hier (Variante 2 " Firmware Update über die Hilfeseite").

Bekannte Fehler mit der Firmware 9.02.14:

- Keine

Router Firmware 9.02.12 (Juni 2018)

Die Firmware ist primär eine verbesserte Version der Firmware 9.02.06 / 9.02.10 und stabilisiert Installationen welche mit FixIP, Port-Weiterleitungen oder DMZ arbeiten.

Alle Centro Business 2.0 die noch nicht auf der Firmware 9.02.06 bzw. FixIP, Port-Weiterleitungen oder DMZ verwenden, werden in den nächsten Wochen automatisch auf die neue Version (9.02.12) aktualisiert. Sie können jedoch die Firmware manuell über die offizielle Centro Business 2.0 Hilfeseite updaten.

Fehlerbehebungen

- Port Forwarding: Im Anwendungsfall von Port-Weiterleitungen auf dem Centro Business 2.0 mit FixIP, arbeiten die Port-Weiterleitungen nach der Firmware-Aktualisierung, sowie nach einem Router-Neustart wieder korrekt.
- DynDNS: Der DynDNS-Service arbeitet nach der Firmware-Aktualisierung, sowie nach einem Router-Neustart wieder korrekt.

Bekannte Fehler mit der Firmware 9.02.12:

- In seltenen Fällen kann sich ein Router mit Werkseinstellung (Inbetriebnahme oder nach Reset), welcher sich über Kupfertechnologie mit dem Internet verbinden will, nicht mit dem Swisscom-Netz synchronisieren. Bitte wenden Sie sich an die SME Hotline.

Router Firmware 9.02.10 (Juni 2018)

Die Firmware ist primär eine verbesserte Version der Firmware 9.02.06 und stabilisiert Installationen welche mit FixIP und DMZ arbeiten.

Alle Centro Business 2.0 die noch nicht auf der Firmware 9.02.06 bzw. FixIP und DMZ verwenden, werden in den nächsten Wochen automatisch auf die neue Version (9.02.10) aktualisiert. Sie können jedoch die Firmware manuell über die offizielle Centro Business 2.0 Hilfeseite updaten.

Fehlerbehebungen

- DMZ: Dass die Business Telefonie im Anwendungsfall «DMZ auf Port 1», nach einem PPP Unterbruch oder Reboot, Registrations- oder Verbindungsprobleme hat, wurde gelöst.
- DMZ: Der Fehler, dass vereinzelt nach einer Firmware-Aktualisierung die DMZ Funktion nicht korrekt startet wurde behoben.
- Weitere Stabilitätsverbesserungen

Bekannte Fehler mit der Firmware 9.02.10:

- DynDNS: Es kann vorkommen, dass der DynDNS-Service gelegentlich unterbrochen wird. Als Workaround kann die DynDNS-Option im Router GUI deaktiviert und wieder aktiviert werden.
- Port Forwarding: Im Anwendungsfall von Port-Weiterleitungen auf dem Centro Business 2.0 mit FixIP, kommt es bei der Firmware-Aktualisierung so wie bei einem Router-Neustart zur Situation, dass die Regeln zwar im Router-Portal sichtbar sind, aber nicht funktionieren. Der Fehler kann behoben werden, indem man die Portweiterleitung im Router-Portal deaktiviert und wieder aktiviert. Durch Vermeidung von einem Router-Neustart kann verhindert werden, dass der Fehlzustand wieder eintritt.

Router Firmware 9.02.06 (April 2018)

Neue Funktionen

Unterstützung von G.fast

G.fast ist die neueste Technologie, mit der wir die Datenübertragungsraten im Kupfer-Festnetz massiv erhöhen können. Der Netzausbau hat erst begonnen und erfolgt kontinuierlich. Verfügbare Bandbreite prüfen

Unterstützung von Premium Call

Gilt nur für my KMU Office und inOne KMU Office

Es können 6 Telefonverbindungen gleichzeitig geführt werden, wenn im Abonnement mindestens 6 Kanäle enthalten sind. Neu können die 2 ISDN Sprachkanäle deaktiviert werden und somit der DECT Basisstation zusätzlich zur Verfügung gestellt werden. Die Anzahl der gleichzeitigen Anrufe sind begrenzt. Die Einstellungen können im Router-Portal unter dem Menüpunkt VoIP/Basic Settings vorgenommen werden. Eine Veränderung der bestehenden Einstellung hat einen Router-Reboot zur Folge.

Gleichzeite Telefonverbindungen pro Technologie	Anzahl Tel.-Kanäle bei Verwendung von ISDN Telefonen	Anzahl Tel.-Kanäle bei Deaktivierung von ISDN
Analog Telefonie (Tel.)	2	2
ISDN Telefonie (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

Manuelle DNS-Server Konfiguration

Im Router-Portal kann neu unter dem Menupunkt "Internet Grundeinstellungen" der manuelle DNS-Modus aktiviert und so ein bevorzugter primärer und sekundärer DNS-Server festgelegt werden. Diese Funktion ermöglicht die Umgehung des neu eingeführten Internet Guard.

Neue Benutzer-Rolle „techadmin“ für die optimale Kundenbetreuung des IT-Partner

Neben den bekannten Benutzer-Rollen „admin“ für lokalen Router-Portal Zugriff und „superadmin“ für den temporären Remote-Zugriff (Freischaltung im Kundencenter), wurde die neue Rolle „techadmin“ angelegt.

Diese Rolle kann nach Freigabe im Routerportal sowohl lokal im LAN, als auch mit Fernzugriff (nur https://) temporär auf das Router-Portal zugreifen. Das zu definierende und fixe Passwort kann initial nur durch den „Admin“ (Kunde/Inhaber) angelegt werden. Er entscheidet, ob er diesen Zugang seinem Vertrauenspartner zur Verfügung stellt und somit von optimaler und sicherer Betreuung profitieren möchte. Der „techadmin“ verfügt über dieselben Rechte wie der Admin, ausser, dass er das „admin“ und „techadmin“ Router-Zugangspasswort nicht einsehen bzw. ändern kann.

Router Remote-Management um zum Beispiel das WLAN zu konfigurieren

Neu bietet sich die Möglichkeit, als „techadmin“ inkl. HTTPS-Verschlüsselung, via Fernzugriff (remote) auf dem Centro Business 2.0 diverse Konfigurationen vorzunehmen.

Zur detaillierten Hilfedokumentation

Wichtige Hinweise:

- Der "admin" muss initial den "techadmin" mit Passwort im Router-Portal anlegen.
- Sowohl der "admin" lokal, als auch der "superadmin" von Remote (via Kundencenter), kann den temporären "techadmin" Remote-Zugang durch setzen der Zugriffsdauer (15, 30, 60 Minuten) aktivieren.
- Es kann gleichzeitig immer nur eine Benutzer-Rolle von Remote auf das Router-Portal zugreifen.
- Aus Sicherheitsgründen wurden dauerhafte Remote-Zugriffsmöglichkeiten abgeschafft.

Vorgehen für "techadmin" der den Fernzugriff aktivieren möchte:

1. Via Kundencenter den Fernzugriff aktivieren und mit dem "superadmin" Zugang auf das Router-Portal zugreifen.
2. Im Menüpunkt "Router" die Zugriffszeit auswählen und speichern. Dadurch wird der „superadmin“ Session gesperrt.
3. Um jetzt als “techadmin“ einzuloggen, muss im Browser die bestehende URL manuell auf https://“WAN-IP“ umgeschrieben werden.
4. Mit Eingabe von „Enter“ wird das Login-Fenster angezeigt. Einloggen mit „techadmin“ und dem Passwort, welches der „admin“ vordefiniert hat.

NAT-Tabellen (LAN & DMZ) unter Diagnose (ausschliesslich für den „superadmin“ und „techadmin“ sichtbar)

Neu können die NAT-Tabellen für LAN und DMZ im Router-Portal unter dem Menüpunkt Diagnose eingesehen und exportiert werden. Sie haben somit die Möglichkeit aktiven Session über die jeweiligen IP's und Port's zu identifizieren und für die Analyse bzw. Entstörung ihres Netzwerkes zu verwenden.

Nähere Informationen über die Funktionsweise von NAT können Sie hier entnehmen.

Fehlerbehebungen

Fehlerbehebungen für Upgrades von 8.06.08:

- Das Probem mit ungewollter Viererkonferenz bei über DECT verbundenen Handapparate und interner Weiterleitung von Anrufen wurde gelöst.
- Verschiedene Einschränkungen bei Verwendung von IPv6 wurden behoben
- Verbindungsabbrüche bei SBcon Telefonie konnten korrigiert werden
- Centro Business 2.0 welche mit IP-Passthrough konfiguriert sind, können sich nach einem DSL Signalunterbuch korrekt mit dem Internet verbinden.
- Centro Business 2.0 die IP-Passthrough ohne aktivem Host konfiguriert haben, verhalten sich korrekt
- Verbessertes Verhalten vom PPP Verbindungsaufbau bei Fiber Anschlüssen
- Diverse Stabilitätsverbesserungen für den BNS Service
- DNS Fehlverhalten in Zusammenhang mit der Internet-Backup Funktion konnte korrigiert werden

Wichtige Empfehlung:
Kunden die in der Vergangenheit den Internet-Backup Stick wegen Serviceeinschränkungen ausser Betrieb genommen hatten, sollen diesen unbedingt wieder am Centro Business 2.0 anschliessen, um im Fall eines Unterbruchs von der Serviceverfügbarkeit über das mobile Netz zu profitieren.

Fehlerbehebungen für Upgrades von 9.01.04:

- Anrufe mit lokalen SIP Credentials über das Gäste-WLAN werden aus Sicherheitsgründen nicht mehr unterstützt.
- Bei Anschlüssen mit fixer IP werden nach einem WAN Reset die Portforwarding Einstellungen korrekt übernommen.
- Konferenzverbindungen intern mit extern funktionieren nun korrekt.
- Diverse Verbindungsprobleme und Unterbrüche (nach ca. 15min) in der Telefonie, sowie Probleme mit der BLF Anzeige wurden behoben.
- Diverse Verbesserungsmassnahmen beim Verbindungsaufbau über Fibre und DSL, sowie DHCP Stabilitätsverbesserungen im lokalen Netz.
- Die automatische Kanalwahl des 5gHz Band arbeitet wieder korrekt.
- Die DMZ funktioniert nach PPP-Verbindungsunterbrüchen wieder korrekt.

Fehlerbehebungen für Upgrades von 9.02.04:

- Das Tastenwahlsignal mit dem Mehrfrequenzwahlverfahren DTMF via DECT-Basisstation wird wieder korrekt übermittelt.

Bekannte Fehler mit der Firmware 9.02.06

- DMZ: Vereinzelnd arbeitet die DMZ-Funktion nach einem FW-Upgrade nicht mehr. Der Fehler kann mit einer Deaktivierung und Reaktivierung im Router Portal behoben werden.
- DynDNS: Es kann vorkommen, dass der DynDNS-Service gelegentlich unterbrochen wird. Als Workaround kann die DynDNS-Option im Router GUI deaktiviert und wieder aktiviert werden.
- Bei einem PPP Session-Unterbruch kommt es vereinzelt vor, dass im Anwendungsfall «DMZ auf Port 1» die dahinterliegende Business Telefonie (PBX@HET sowie SIP Phones bei Smart Business Connect und InOne KMU) Probleme bei der Registration bzw. dem Telefonieren hat. Das Problem ist auch auf früheren Firmware-Versionen vorhanden und kann durch einen Router-Neustart korrigiert werden.
- Betrifft nur Centro Business 2.0 welche aktuell mit Firmware 9.01.04 laufen:
  Drückt man im Router-Portal (192.168.1.1), unter "Router-> Firmware" den Update-Button "Nach Aktualisierung suchen", findet der Router zwar die neue Firmware Version (9.02.06), sie lässt sich aber nicht installieren. Es erscheint fälschlicherweise die Nachricht "Firmware ist auf dem aktuellen Stand". Alternativ kann die Firmware als Datei aber lokal ausgewählt und installiert werden. Alternativ kann mit einem Reset auf die Werkseinstellungen das Firmware-Update auch automatisch forciert werden.

9.02.04 (März 2018)

Neue Funktionen

Unterstützung von G.fast

G.fast ist die neueste Technologie, mit der wir die Datenübertragungsraten im Kupfer-Festnetz massiv erhöhen können. Der Netzausbau hat erst begonnen und erfolgt kontinuierlich. Verfügbare Bandbreite prüfen

Unterstützung von Premium Call

Gilt nur für my KMU Office und inOne KMU Office

Es können 6 Telefonverbindungen gleichzeitig geführt werden, wenn im Abonnement mindestens 6 Kanäle enthalten sind. Neu können die 2 ISDN Sprachkanäle deaktiviert werden und somit der DECT Basisstation zusätzlich zur Verfügung gestellt werden. Die Anzahl der gleichzeitigen Anrufe sind begrenzt. Die Einstellungen können im Router-Portal unter dem Menüpunkt VoIP/Basic Settings vorgenommen werden. Eine Veränderung der bestehenden Einstellung hat einen Router-Reboot zur Folge.

Gleichzeite Telefonverbindungen pro Technologie	Anzahl Tel.-Kanäle bei Verwendung von ISDN Telefonen	Anzahl Tel.-Kanäle bei Deaktivierung von ISDN
Analog Telefonie (Tel.)	2	2
ISDN Telefonie (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

Manuelle DNS-Server Konfiguration

Im Router-Portal kann neu unter dem Menupunkt "Internet Grundeinstellungen" der manuelle DNS-Modus aktiviert und so ein bevorzugter primärer und sekundärer DNS-Server festgelegt werden. Diese Funktion ermöglicht die Umgehung des neu eingeführten Internet Guard.

Neue Benutzer-Rolle „techadmin“ für die optimale Kundenbetreuung des IT-Partner

Neben den bekannten Benutzer-Rollen „admin“ für lokalen Router-Portal Zugriff und „superadmin“ für den temporären Remote-Zugriff (Freischaltung im Kundencenter), wurde die neue Rolle „techadmin“ angelegt.

Diese Rolle kann nach Freigabe im Routerportal sowohl lokal im LAN, als auch mit Fernzugriff (nur https://) temporär auf das Router-Portal zugreifen. Das zu definierende und fixe Passwort kann initial nur durch den „Admin“ (Kunde/Inhaber) angelegt werden. Er entscheidet, ob er diesen Zugang seinem Vertrauenspartner zur Verfügung stellt und somit von optimaler und sicherer Betreuung profitieren möchte. Der „techadmin“ verfügt über dieselben Rechte wie der Admin, ausser, dass er das „admin“ und „techadmin“ Router-Zugangspasswort nicht einsehen bzw. ändern kann.

Router Remote-Management um zum Beispiel das WLAN zu konfigurieren

Neu bietet sich die Möglichkeit, als „techadmin“ inkl. HTTPS-Verschlüsselung, via Fernzugriff (remote) auf dem Centro Business 2.0 diverse Konfigurationen vorzunehmen.

Zur detaillierten Hilfedokumentation

Wichtige Hinweise:

- Der "admin" muss initial den "techadmin" mit Passwort im Router-Portal anlegen.
- Sowohl der "admin" lokal, als auch der "superadmin" von Remote (via Kundencenter), kann den temporären "techadmin" Remote-Zugang durch setzen der Zugriffsdauer (15, 30, 60 Minuten) aktivieren.
- Es kann gleichzeitig immer nur eine Benutzer-Rolle von Remote auf das Router-Portal zugreifen.
- Aus Sicherheitsgründen wurden dauerhafte Remote-Zugriffsmöglichkeiten abgeschafft.

Vorgehen für "techadmin" der den Fernzugriff aktivieren möchte:

1. Via Kundencenter den Fernzugriff aktivieren und mit dem "superadmin" Zugang auf das Router-Portal zugreifen.
2. Im Menüpunkt "Router" die Zugriffszeit auswählen und speichern. Dadurch wird der „superadmin“ Session gesperrt.
3. Um jetzt als “techadmin“ einzuloggen, muss im Browser die bestehende URL manuell auf https://“WAN-IP“ umgeschrieben werden.
4. Mit Eingabe von „Enter“ wird das Login-Fenster angezeigt. Einloggen mit „techadmin“ und dem Passwort, welches der „admin“ vordefiniert hat.

NAT-Tabellen (LAN & DMZ) unter Diagnose (ausschliesslich für den „superadmin“ und „techadmin“ sichtbar)

Neu können die NAT-Tabellen für LAN und DMZ im Router-Portal unter dem Menüpunkt Diagnose eingesehen und exportiert werden. Sie haben somit die Möglichkeit aktiven Session über die jeweiligen IP's und Port's zu identifizieren und für die Analyse bzw. Entstörung ihres Netzwerkes zu verwenden.

Nähere Informationen über die Funktionsweise von NAT können Sie hier entnehmen.

Fehlerbehebungen

- Das Problem in der Zwischenversion 9.01.02, dass Telefonate via HD-Phone Sarnen und dem Yealink T46G nach 15 - 30 Minuten unterbrochen wurde, ist gelöst
- Das Problem mit ungewollter Viererkonferenz bei, über DECT verbundenen Handapparate und interner Weiterleitung von Anrufen wurde gelöst
- Verschiedene Einschränkungen bei Verwendung von IPv6 wurden behoben
- Verbindungsabbrüche bei SBcon Telefonie konnten korrigiert werden
- Centro Business 2.0 welche mit IP-Passthrough konfiguriert sind, können sich nach einem DSL Signalunterbuch korrekt mit dem Internet verbinden
- Centro Business 2.0 die IP-Passthrough ohne aktiven Host konfiguriert haben, verhalten sich korrekt
- Verbessertes Verhalten vom PPP Verbindungsaufbau bei Fiber Anschlüssen
- DNS Fehlverhalten in Zusammenhang mit der Internet-Backup Funktion konnte korrigiert werden
- Diverse Stabilitätsverbesserungen für den BNS Service

Wichtige Empfehlung:
Kunden die in der Vergangenheit den Internet-Backup Stick wegen Serviceeinschränkungen ausser Betrieb genommen hatten, sollen diesen unbedingt wieder am Centro Business 2.0 anschliessen, um im Fall eines Unterbruchs von der Serviceverfügbarkeit über das mobile Netz zu profitieren.

Bekannte Fehler mit der Firmware 9.02.04

- Die automatische Kanalwahl des 5gHz Band arbeitet nicht korrekt. Der Centro Business 2.0 wählt mit der Firmware 9.01.04 immer den Kanal 36. Wenn die WLAN Verbindungsqualität durch viele andere WLAN-Signale gestört ist und Probleme mit der Internetverbindung generiert, empfiehlt es sich den Kanal manuell im Router-Portal zu manipulieren.
- Betrifft nur Centro Business 2.0 welche aktuell mit Firmware 9.01.04 laufen:
  Drückt man im Router-Portal (192.168.1.1), unter "Router-> Firmware" den Update-Button "Nach Aktualisierung suchen", findet der Router zwar die neue Firmware Version (9.02.06), sie lässt sich aber nicht installieren. Es erscheint fälschlicherweise die Nachricht "Firmware ist auf dem aktuellen Stand". Alternativ kann die Firmware als Datei aber lokal ausgewählt und installiert werden. Alternativ kann mit einem Reset auf die Werkseinstellungen das Firmware-Update auch automatisch forciert werden.

9.01.04 (September 2017)

Neue Funktionen

Unterstützung von G.fast

G.fast ist die neueste Technologie, mit der wir die Datenübertragungsraten im Kupfer-Festnetz massiv erhöhen können. Der Netzausbau hat erst begonnen und erfolgt kontinuierlich. Verfügbare Bandbreite prüfen

Unterstützung von Premium Call

Gilt nur für my KMU Office und inOne KMU Office

Es können 6 Telefonverbindungen gleichzeitig geführt werden, wenn im Abonnement mindestens 6 Kanäle enthalten sind. Neu können die 2 ISDN Sprachkanäle deaktiviert werden und somit der DECT Basisstation zusätzlich zur Verfügung gestellt werden. Die Anzahl der gleichzeitigen Anrufe sind begrenzt. Die Einstellungen können im Router-Portal unter dem Menüpunkt VoIP/Basic Settings vorgenommen werden. Eine Veränderung der bestehenden Einstellung hat einen Router-Reboot zur Folge.

Gleichzeite Telefonverbindungen pro Technologie	Anzahl Tel.-Kanäle bei Verwendung von ISDN Telefonen	Anzahl Tel.-Kanäle bei Deaktivierung von ISDN
Analog Telefonie (Tel.)	2	2
ISDN Telefonie (ISDN)	2	0
DECT CAT-iq	2 (HD) Voice	2 (HD Voice) + 2 (Voice)

Manuelle DNS-Server Konfiguration

Im Router-Portal kann neu unter dem Menupunkt "Internet Grundeinstellungen" der manuelle DNS-Modus aktiviert und so ein bevorzugter primärer und sekundärer DNS-Server festgelegt werden. Diese Funktion ermöglicht die Umgehung des neu eingeführten Internet Guard.

Neue Benutzer-Rolle „techadmin“ für die optimale Kundenbetreuung des IT-Partner

Neben den bekannten Benutzer-Rollen „admin“ für lokalen Router-Portal Zugriff und „superadmin“ für den temporären Remote-Zugriff (Freischaltung im Kundencenter), wurde die neue Rolle „techadmin“ angelegt.

Diese Rolle kann nach Freigabe im Routerportal sowohl lokal im LAN, als auch mit Fernzugriff (nur https://) temporär auf das Router-Portal zugreifen. Das zu definierende und fixe Passwort kann initial nur durch den „Admin“ (Kunde/Inhaber) angelegt werden. Er entscheidet, ob er diesen Zugang seinem Vertrauenspartner zur Verfügung stellt und somit von optimaler und sicherer Betreuung profitieren möchte. Der „techadmin“ verfügt über dieselben Rechte wie der Admin, ausser, dass er das „admin“ und „techadmin“ Router-Zugangspasswort nicht einsehen bzw. ändern kann.

Router Remote-Management um zum Beispiel das WLAN zu konfigurieren

Neu bietet sich die Möglichkeit, als „techadmin“ inkl. HTTPS-Verschlüsselung, via Fernzugriff (remote) auf dem Centro Business 2.0 diverse Konfigurationen vorzunehmen.

Zur detaillierten Hilfedokumentation

Wichtige Hinweise:

- Der "admin" muss initial den "techadmin" mit Passwort im Router-Portal anlegen.
- Sowohl der "admin" lokal, als auch der "superadmin" von Remote (via Kundencenter), kann den temporären "techadmin" Remote-Zugang durch setzen der Zugriffsdauer (15, 30, 60 Minuten) aktivieren.
- Es kann gleichzeitig immer nur eine Benutzer-Rolle von Remote auf das Router-Portal zugreifen.
- Aus Sicherheitsgründen wurden dauerhafte Remote-Zugriffsmöglichkeiten abgeschafft.

Vorgehen für "techadmin" der den Fernzugriff aktivieren möchte:

1. Via Kundencenter den Fernzugriff aktivieren und mit dem "superadmin" Zugang auf das Router-Portal zugreifen.
2. Im Menüpunkt "Router" die Zugriffszeit auswählen und speichern. Dadurch wird der „superadmin“ Session gesperrt.
3. Um jetzt als “techadmin“ einzuloggen, muss im Browser die bestehende URL manuell auf https://“WAN-IP“ umgeschrieben werden.
4. Mit Eingabe von „Enter“ wird das Login-Fenster angezeigt. Einloggen mit „techadmin“ und dem Passwort, welches der „admin“ vordefiniert hat.

NAT-Tabellen (LAN & DMZ) unter Diagnose (ausschliesslich für den „superadmin“ und „techadmin“ sichtbar)

Neu können die NAT-Tabellen für LAN und DMZ im Router-Portal unter dem Menüpunkt Diagnose eingesehen und exportiert werden. Sie haben somit die Möglichkeit aktiven Session über die jeweiligen IP's und Port's zu identifizieren und für die Analyse bzw. Entstörung ihres Netzwerkes zu verwenden.

Nähere Informationen über die Funktionsweise von NAT können Sie hier entnehmen.

Fehlerbehebungen

- Das Problem mit ungewollter Viererkonferenz bei, über DECT verbundenen Handapparate und interner Weiterleitung von Anrufen wurde gelöst.
- Verschiedene Einschränkungen bei Verwendung von IPv6 wurden behoben
- Verbindungsabbrüche bei SBcon Telefonie konnten korrigiert werden
- Centro Business 2.0 welche mit IP-Passthrough konfiguriert sind, können sich nach einem DSL Signalunterbuch korrekt mit dem Internet verbinden.
- Centro Business 2.0 die IP-Passthrough ohne aktivem Host konfiguriert haben, verhalten sich korrekt
- Verbessertes Verhalten vom PPP Verbindungsaufbau bei Fiber Anschlüssen
- DNS Fehlverhalten in Zusammenhang mit der Internet-Backup Funktion konnte korrigiert werden
- Diverse Stabilitätsverbesserungen für den BNS Service

Bekannte Fehler mit der Firmware 9.01.04

- Die automatische Kanalwahl des 5gHz Band arbeitet nicht korrekt. Der Centro Business 2.0 wählt mit der Firmware 9.01.04 immer den Kanal 36. Wenn die WLAN Verbindungsqualität durch viele andere WLAN-Signale gestört ist und Probleme mit der Internetverbindung generiert, empfiehlt es sich den Kanal manuell im Router-Portal zu manipulieren.
- Betrifft nur Centro Business 2.0 welche aktuell mit Firmware 9.01.04 laufen:
  Drückt man im Router-Portal (192.168.1.1), unter "Router-> Firmware" den Update-Button "Nach Aktualisierung suchen", findet der Router zwar die neue Firmware Version (9.02.06), sie lässt sich aber nicht installieren. Es erscheint fälschlicherweise die Nachricht "Firmware ist auf dem aktuellen Stand". Alternativ kann die Firmware als Datei aber lokal ausgewählt und installiert werden. Alternativ kann mit einem Reset auf die Werkseinstellungen das Firmware-Update auch automatisch forciert werden.