COMET Cloud je unikátní platforma, která umožňuje sběr dat, ukládání dat a analýzu dat poskytovaných měřicími přístroji COMET.

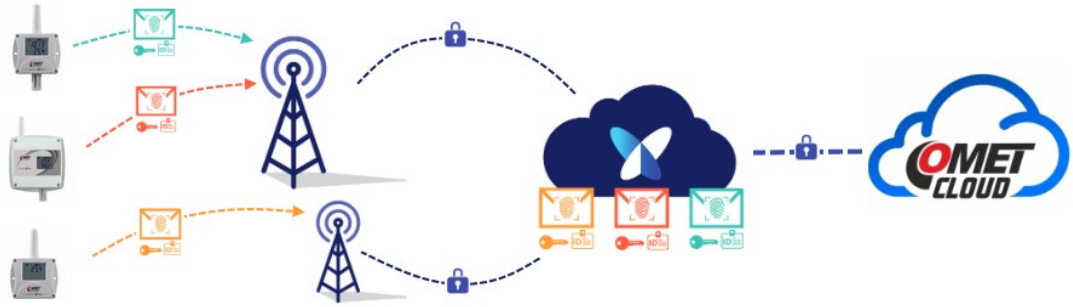
Ochrana vašich osobních údajů a naměřených hodnot je pro nás důležitá. Veškeré ukládání a zpracování dat v systému COMET Cloud probíhá podle nejvyšších standardů a zásad bezpečnosti a zabezpečení. Používáme pouze IT infrastrukturu třetích stran, která tyto vysoké standardy splňuje.

Tento dokument obsahuje všechny důležité informace o zabezpečení COMET Cloud a ochraně vašich dat. Dokument popisuje zabezpečení COMET Cloud pro senzory COMET IoT využívající Sigfox, LoRaWAN, WiFi senzory, webové senzory a bezdrátové IoT dataloggery s vestavěným GSM modemem nebo LTE modemem.

Máte-li jakýkoli dotaz, neváhejte se na nás obrátit.

Jak vypadá řetězec přenosu dat?

IoT senzory s výstupem do sítě Sigfox



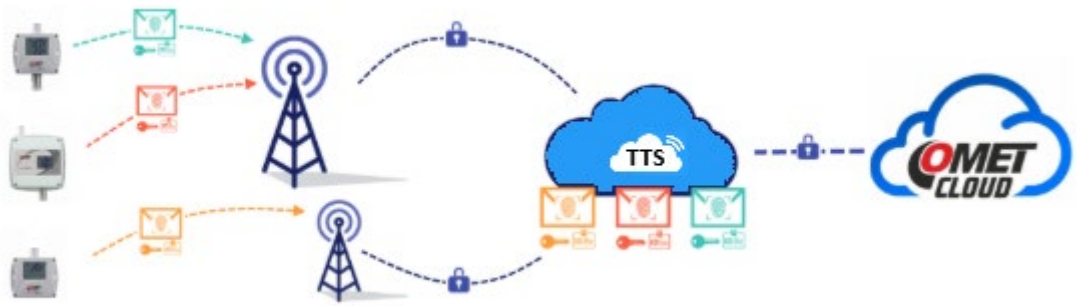
Senzory COMET IoT odesílají v nastavených intervalech malé datové zprávy obsahující naměřené hodnoty a stavová data senzoru. Tyto zprávy přijímají základnové stanice Sigfox (BTS). Lze využít infrastrukturní BTS nebo lokální BTS instalovanou koncovým uživatelem. Data z BTS jsou bezpečně přenášena do infrastruktury Sigfox Cloud. V této infrastruktuře se ověřuje pravost zprávy. Po úspěšném ověření jsou zprávy prostřednictvím zabezpečeného připojení HTTPS přeneseny do COMET Cloud. Příchozí zprávy jsou v systému COMET Cloud dekódovány, zpracovány a uloženy.

Jako rádiový přenosový kanál se používá bezlicenční pásmo 868 MHz. Komunikace je úzkopásmová s frekvenčním přeskakováním. Díky tomu jsou přenosy dat vysoce odolné vůči rušení. Vzhledem k frekvenčnímu přeskakování je technicky velmi obtížné zprávu zachytit potenciálním útočníkem.

Pravost zpráv je zajištěna jejich podepisováním. Každý IoT senzor obsahuje jedinečný tajný klíč. Tento klíč se používá k podepisování každé odesílané zprávy. Datová zpráva obsahuje také pořadové číslo. Toto číslo poskytuje ochranu proti útoku typu „replay“.

Díky ověření podpisu je zajištěn původ naměřených dat. Podpis brání útočníkovi v odesílání škodlivých zpráv.

IoT snímače s výstupem do sítě LoRaWAN®



Senzory COMET IoT odesílají v definovaných intervalech malé datové zprávy obsahující naměřené hodnoty a stavová data zařízení. Tyto zprávy přijímají brány LoRaWAN®. Brány může provozovat přímo uživatel nebo lze využít infrastrukturu třetích stran. Brána přenáší přijatá rádiová data do síťového serveru LoRaWAN® v prostředí The Things Stack (TTS) prostřednictvím zabezpečeného připojení TLS. V prostředí TTS se ověřuje pravost a integrita zprávy. Zpráva je poté předána do COMET Cloud prostřednictvím zabezpečeného kanálu k dalšímu zpracování.

Pro rádiový přenos se používá bezlicenční pásmo 868 MHz. Komunikace je širokopásmová (spread spectrum), což zajišťuje vysokou odolnost vůči rušení i v náročném RF prostředí.

Rádiový přenos LoRaWAN® používá jedinečné kryptografické klíče k šifrování přenášených dat a ověřování zpráv. Přenos navíc poskytuje ochranu proti „replay attack“. Díky využití těchto mechanismů zajišťují IoT senzory vysokou úroveň zabezpečení i pro nejnáročnější aplikace.

WiFi senzory

Senzory COMET WiFi odesílají data do COMET Cloud v nastavených intervalech prostřednictvím běžné WiFi infrastruktury 2,4 GHz. WiFi senzory jsou vybaveny vlastní nevolatilní pamětí pro vzorky, které nelze odeslat v případě výpadku připojení WiFi nebo ISP.

WiFi senzory podporují nejmodernější bezpečnostní standardy WLAN pro WiFi konektivitu. Kromě obvyklých standardů, jako jsou WEP a WPA/WPA2, podporují WiFi senzory i nejnovější standardy WPA3, WPA2 PMF (Protected Management Frames) a WPA2-EAP. Veškerá datová komunikace mezi WiFi senzory a COMET Cloud je šifrována a přenášena prostřednictvím protokolu HTTPS. Každá komunikace mezi WiFi senzorem a COMET Cloud je ověřována vzájemnou autentizací.

Díky použití osvědčených bezpečnostních standardů poskytují WiFi senzory vysokou úroveň ochrany proti potenciálnímu útočníkovi, a to jak z hlediska ochrany obsahu dat, tak ochrany před odesíláním škodlivých dat do COMET Cloud.

Web Senzory (t-line, p-line, h-line)

Webové senzory COMET odesílají data do COMET Cloud prostřednictvím ethernetové infrastruktury. Naměřené hodnoty jsou odesílány pomocí protokolu SOAP přenášeného přes HTTP.
Pravost přenosu dat je zajištěna jedinečným vstupním bodem pro každý webový senzor. Tento vstupní bod se generuje ve webovém rozhraní COMET Cloud a musí být vložen do každého webového senzoru samostatně. Pravost zpráv z webových senzorů je zajištěna, pokud je jedinečný vstupní bod uchován v tajnosti.

COMET Cloud je vybaven automatickým systémem ochrany integrity příchozích dat. Tok dat ze zařízení je pozastaven, pokud je zjištěna neobvyklá aktivita, například kratší interval odesílání, než je povoleno.

Bezdrátové IoT dataloggery s vestavěným GSM modemem nebo LTE modemem

Bezdrátové IoT dataloggery s vestavěným GSM modemem nebo LTE modemem používají pro přenos dat HTTP komunikaci prostřednictvím připojení GSM nebo LTE. Bezdrátové IoT dataloggery jsou vybaveny vlastní nevolatilní pamětí, do které se ukládají vzorky při výpadku sítě GSM nebo LTE. Tuto paměť lze využít k optimalizaci přenosů dat ve spojení s úsporou energie z interní baterie.

Ochranu obsahu dat zajišťuje síť GSM nebo LTE. Příchozí zprávy do COMET Cloud jsou před zpracováním kontrolovány z hlediska integrity.

Jaká data jsou v COMET Cloud ukládána?

Kromě naměřených hodnot ze zařízení se v COMET Cloud ukládají také e-mailové adresy. Tyto adresy se používají pro zasílání alarmových upozornění ze zařízení nebo servisních informací cloudové služby. Tyto e-maily nejsou používány k marketingovým účelům jakéhokoli druhu. Pokud je používána mobilní aplikace pro zasílání zpráv, ukládá COMET Cloud jedinečnou identifikaci každého zařízení Android nebo iOS. COMET Cloud neukládá žádné další osobní údaje. Ukládaná data se liší podle modelu zařízení:

IoT senzory s výstupem do sítí Sigfox a LoRaWAN®

- Naměřené hodnoty
- Stav zařízení a alarmové stavy
- Konfigurace zařízení
- Lokalizační údaje

Lokalizace zařízení Sigfox je založena na triangulaci z BTS. Přesnost lokalizace závisí na počtu BTS v dosahu a není lepší než úroveň ulice nebo městské části. Účelem lokalizačních údajů je zobrazení polohy zařízení na mapě. Polohu na mapě může koncový uživatel v případě potřeby upravit.

WiFi senzory

- Naměřené hodnoty
- Stav zařízení a alarmové stavy
- Lokální IP adresa

Lokální IP adresa zařízení je přenášena ze zařízení. Účelem této IP adresy je umožnit otevření webové stránky zařízení z prostředí COMET Cloud. Z WiFi senzorů se do COMET Cloud nepřenášejí žádné další informace související se síťovou infrastrukturou. Externí IP adresy datových připojení z úspěšně autentizovaných WiFi senzorů se nezaznamenávají.

Webové senzory (t-line, p-line, h-line)

- Naměřené hodnoty
- Stav zařízení a alarmové stavy

Webové senzory neposkytují žádná jiná data než ta uvedená výše. Externí IP adresy datových připojení z úspěšně autentizovaných zpráv se nezaznamenávají.

Bezdrátové IoT dataloggery s vestavěným GSM modemem nebo LTE modemem

- Naměřené hodnoty
- Stav zařízení a alarmové stavy

Veškerá shromažďovaná data z bezdrátových IoT dataloggerů jsou uvedena výše. Externí IP adresy datových připojení z úspěšně autentizovaných zpráv se nezaznamenávají. Lokalizační údaje ze sítě GSM se neshromažďují.
Datová komunikace mezi COMET Cloud a webovým prohlížečem může být z provozních důvodů zaznamenávána, aby byl zajištěn chod systému. Tato komunikace se nepoužívá ke sledování chování koncových uživatelů.

Kde jsou má data uložena?

COMET Cloud využívá pro ukládání a zpracování dat infrastrukturu cloudových služeb Microsoft Azure. Pro COMET Cloud se používají datová centra umístěná v zemích EU. Používaná datová centra jsou certifikována podle normy ISO/IEC 27001:2022.

Jsou má data v bezpečí?

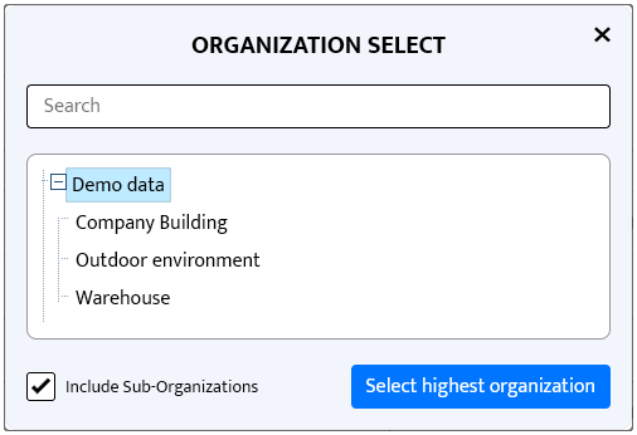
COMET Cloud je navržen jako služba s vysokou dostupností. Pro provoz COMET Cloud se používá několik serverových clusterů včetně zálohování mimo lokalitu. Stav služeb COMET Cloud je průběžně monitorován automatizovaným systémem a oprávněnými zaměstnanci společnosti COMET System s.r.o. Jakákoli odchylka dostupnosti služeb je řešena okamžitě.

Při ukládání nově přijatých naměřených hodnot nejsou starší naměřené hodnoty přepisovány. Naměřené hodnoty jsou ukládány společně s časovými razítky a alarmovými stavy. To umožňuje zobrazit všechny hodnoty jako časový průběh.
COMET Cloud je poskytován jako služba placená formou ročního předplatného. Nově zakoupené IoT senzory využívající Sigfox jsou dodávány s ročním předplatným. Ostatní modely jsou dodávány se třemi měsíci bezplatného předplatného. Předplatné pro každé zařízení lze prodloužit zakoupením kreditů. Po vypršení předplatného zařízení je příjem dat ze zařízení pozastaven.

Ochrana soukromí při přenosech dat mezi COMET Cloud a internetovým prohlížečem je zajištěna připojením HTTPS. COMET Cloud používá důvěryhodný certifikát vydaný společností DigiCert Inc.

Kdo má přístup k mým uloženým datům?

Přístup k datům mají osoby schválené vlastníkem zařízení. Přístup k datům mají také pracovníci společnosti COMET System s.r.o., kteří poskytují technickou podporu pro správnou funkci COMET Cloud. COMET System s.r.o. neposkytuje přístup k datům koncových uživatelů třetím stranám.



Zařízení COMET Cloud a uživatelské účty jsou uspořádány ve stromové struktuře. Uživatel může zobrazovat zařízení ve stejné nebo nižší větvi organizační struktury. Počet uživatelských účtů pro každou organizaci není omezen.

COMET Cloud využívá model řízení přístupu na základě rolí (Role-Based Access Control – RBAC). Tento model umožňuje:

- definovat různé úrovně oprávnění,
- omezit přístup pouze na vybraná zařízení nebo organizační jednotky,
- řídit, které akce může uživatel provádět (např. konfigurace zařízení, správa alarmů, správa uživatelů nebo zobrazení dat).

Role a jejich oprávnění jsou definovány systémem COMET Cloud. Vlastník účtu s administrátorským oprávněním rozhoduje o přidělení jednotlivých rolí konkrétním podřízeným uživatelům.
Systém je navržen tak, aby každý uživatel měl přístup pouze k funkcím a zařízením nezbytným pro svou práci (princip minimálních oprávnění).
Rozsah rolí může být aktualizován v rámci vývoje systému a vždy odpovídá aktuální verzi služby.

Jaká související legislativa upravuje ochranu dat?

Data koncových uživatelů jsou chráněna právními předpisy České republiky o ochraně osobních údajů. Tyto právní předpisy jsou harmonizovány s právem EU.

Jaké certifikace jsou k dispozici?

Datová centra jsou certifikována podle normy ISO/IEC 27001:2022.

Interní procesy ve společnosti COMET System s.r.o. jsou certifikovány podle systému řízení kvality ISO 9001:2015.

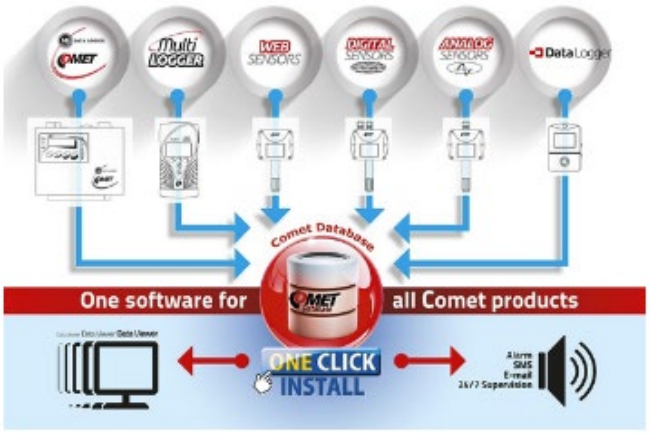
Jak bezpečně používat zařízení ve vlastní síťové infrastruktuře?

WiFi senzory a webové senzory používají pro přenos dat do COMET Cloud síťovou infrastrukturu koncového uživatele. Pro zabezpečení přenosů dat ze zařízení do cloudu se doporučují následující opatření.

Při finálním nasazení se doporučuje povolit zabezpečení zařízení, aby byla zařízení chráněna před neoprávněným přístupem. Dodržujte prosím doporučení IT bezpečnosti uvedená v návodu k WiFi senzorům.

Nemohu používat cloudové služby třetích stran. Jaké mám možnosti?

Pro zákazníky, kteří z bezpečnostních důvodů nemohou využívat cloudové služby třetích stran, nebo pro uživatele, kteří chtějí provozovat systém sběru dat na vlastní serverové infrastruktuře, je k dispozici řešení COMET Database. COMET Database je řešení využívající databázový server Microsoft SQL jako úložiště dat a software Viewer nainstalovaný na klientských stanicích.



Řešení COMET Database umožňuje sběr dat z více typů zařízení COMET, včetně webových senzorů, WiFi senzorů a bezdrátových IoT dataloggerů.