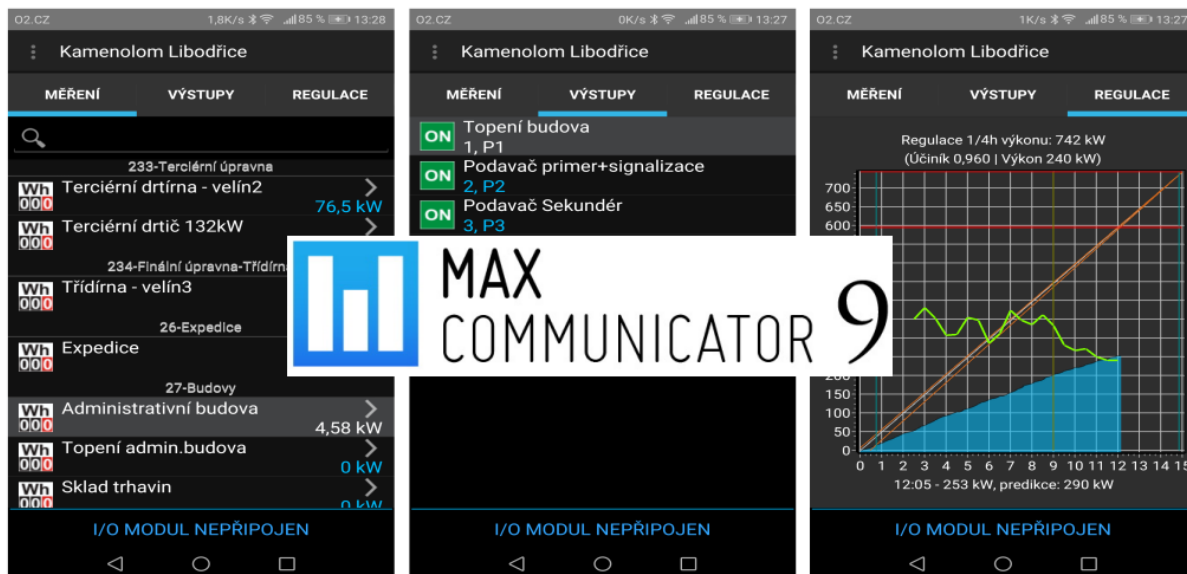


Aplikace „Max Communicator“ pro mobilní telefony



Oblast použití

Aplikace pro energetický management podniků, provozů a institucí...

Bližší specifikace

S pomocí této aplikace lze rozšířit stávající podnikový systém měření a regulace odběrového profilu o dálkový dohled přes mobilní telefon. Přes tuto aplikaci lze i na cestách nebo z domova rychle zkontrolovat **aktuální provozní stav podniku**, jako např. průběh regulace 1/4h výkonu, účinníku, denní limit spotřeby zemního plynu, provozní stav regulačních výstupů nebo aktuální hodnoty výkonů všech měřených obvodů.

Aplikací lze nahlédnout i do **historie spotřeby elektrické energie**, plynu, vody, tepla, dále vyhodnotit průběh teplot, napětí, proudů nebo zjistit rizikové události jako přetížení, výpadky napětí, překročení rezervované kapacity atd. - u jedné nebo až stovek provozoven...

Aplikace získává všechny údaje ze **serveru „MaxComm“**, který je v režii a plně pod kontrolou vlastníka (uživatelé) systému a to včetně dat. **K funkci aplikace není tedy potřeba žádný veřejný „cloud“** nebo jiné sdílené služby. Více informací o struktuře „**klient-server**“ systému „**Max Communicator**“ najdete na webu výrobce **PK-ELSYS**, který vyrábí a dodává všechny klíčové komponenty.

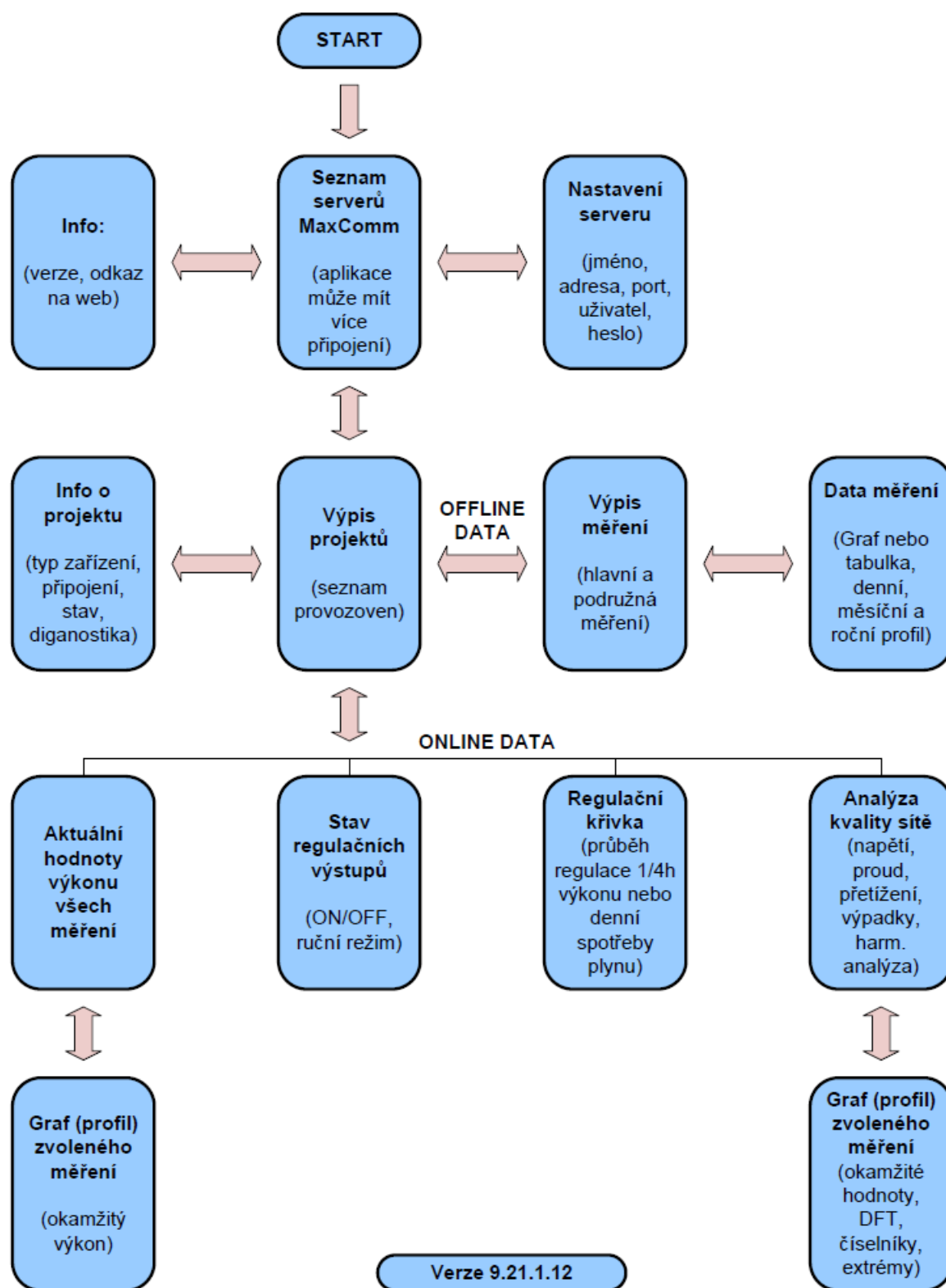
Aplikace ani její provoz není zpoplatněn, nenachází se v ní **žádné reklamy** a **nesbírá žádná data o uživateli**. Licenční podmínky užití aplikace je vázáno na hardware a software od výrobce **PK-ELSYS**. Je zakázáno aplikaci používat jiným způsobem!

1 Obsah

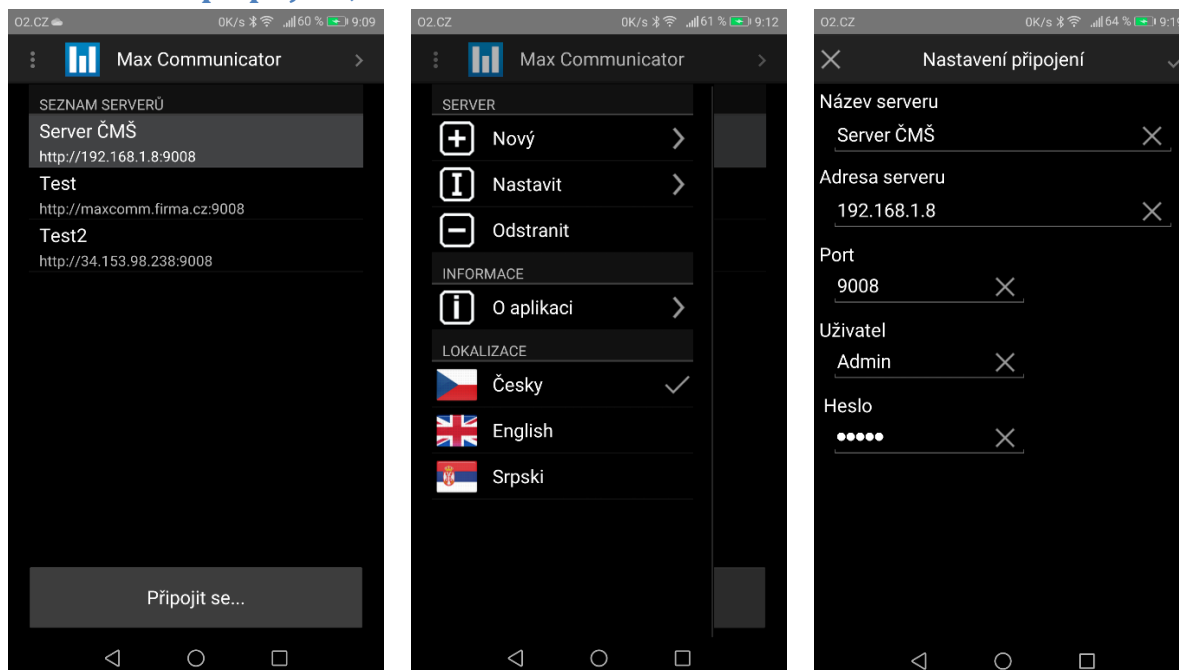
2	Struktura mobilní aplikace Max Communicator.....	3
2.1	Seznam připojení, serverů MaxComm	4
2.2	Výpis projektů.....	5
2.3	Výpis měření.....	7
2.4	Data měření.....	8
2.4.1	Elektřina, předávací měření, odběr	8
2.4.2	Elektřina, podružné měření.....	9
2.4.3	Zemní plyn	10
2.4.4	Měření teploty.....	10
2.4.5	Obecné měření, např přeprava materiálu.....	11
2.4.6	Měření proudového zatížení	11
2.4.7	Analýza kvality napájecí sítě	12
2.4.8	Odečet všech měření.....	12
2.5	Aktuální hodnoty měření (online)	13
2.5.1	Aktuální hodnoty měření elektroměru EME319	14
3	Topologie a bezpečnost systému	16
3.1	Zabezpečení systému proti neoprávněnému přístupu	17
3.1.1	Zabezpečení na úrovni aplikace	17
3.1.2	Zabezpečení přístupového bodu	17
4	Instalace.....	18
4.1	Příprava serveru MaxComm	18
4.2	Konfigurace přístupového bodu	21
4.2.1	Varianta komunikace pomocí „předávaného“ portu	21
4.2.2	Varianta komunikace pomocí VPN	23
4.3	Instalace a konfigurace aplikace na telefonu	25
5	Výrobce aplikace	27

Poslední úpravy: 26.1.2021

2 Struktura mobilní aplikace Max Communicator



2.1 Seznam připojení, serverů MaxComm



Po spuštění aplikace se zobrazí uživatelem předdefinovaný seznam serverů. Po instalaci aplikace je samozřejmě seznam prázdný a je třeba nějaký přidat. Vlevo nahoře se nachází tlačítko pro zobrazení menu – viz obrázek uprostřed...

Formulář záznamu serveru obsahuje tyto údaje:

- **Název serveru** – libovolný text (*raději kratší*)
- **Adresa serveru** – zde vložte adresu HTTP serveru MaxComm, ke kterému se bude aplikace připojovat (*více info – viz Instalace...*)
- **Port** – číslo portu, na kterém je HTTP server MaxComm provozován
- **Uživatel** – přihlašovací jméno uživatele (*účet vytvoříte v desktopové aplikaci MaxComm*)
- **Heslo** – přihlašovací heslo uživatele (*nenechávejte žádné účty bez hesla!*)

Připojení na HTTP server MaxComm samozřejmě předchází jeho instalace a konfigurace. Toto je komplexnější proces, kterému se věnuje samostatná kapitola „*Instalace...*“.

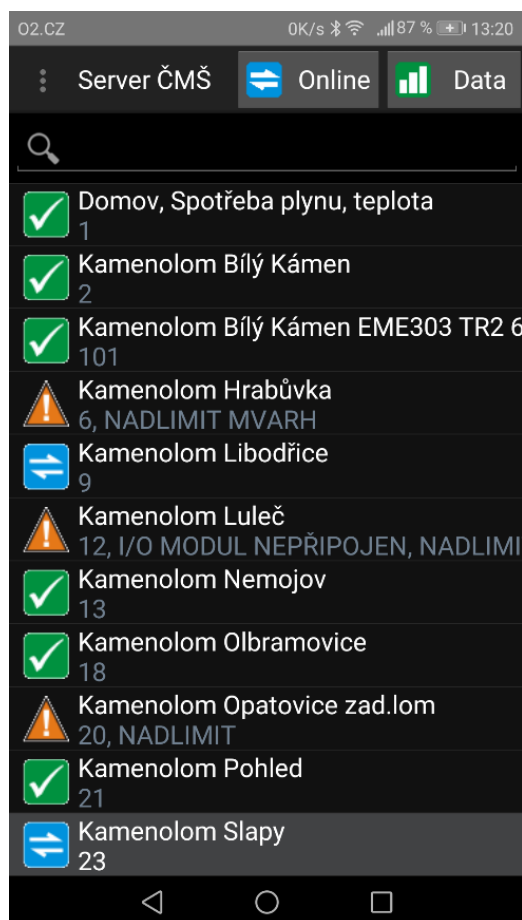
Aplikaci lze přepnout do těchto jazyků:

- **Česky**
- **Anglicky**
- **Srbsky**

Po kliknutí na tlačítko „*Připojit se...*“ se aplikace pokusí připojit k vybranému serveru. V případě úspěchu, se aplikace přepne na „*Výpis projektů*“, které se po připojení načtou z tohoto serveru...

2.2 Výpis projektů

Po úspěšném připojení k HTTP serveru MaxComm, aplikace stáhne výpis všech projektů vytvořených na serveru, ke kterým má přihlášený uživatel přístup:



Projektem se rozumí soubor údajů na serveru vztahující se např. k jedné **provozovně**. Ikona u projektu vlevo indikuje poslední známý **stav projektu**:

	Stav neznámý	Projekt byl vytvořen nebo importován a nemá zatím definovaný žádný status.
	Vše OK	Poslední spojení se zařízením (<i>spojení mezi serverem MaxComm a zařízením</i>) proběhlo v pořádku a nebyly zjištěny žádné závady.
	Připojení se nezdařilo	Poslední pokus o připojení k zařízení selhal.
	Nějaký problém	Při posledním připojení k zařízení (*) byly zjištěny problémy na zařízení nebo diagnostika dat hlásí nějaká varování, např. překročení limitu odběru, špatný účinník, výpadky měření apod.
	Projekt je online	Projekt je nyní k zařízení připojen – může připojit i jiný uživatel nebo sám server při automatickém stahování dat ze zařízení.
	Projekt se upravuje	Nějaký uživatel tento projekt právě upravuje (<i>přes desktopovou aplikaci</i>) a není možné tento projekt uvést do stavu online.

(*) **Zařízení** ... obecné označení pro hardware (např. [ATS-C120](#)), který zajišťuje měření a regulaci. Zde v tomto hardware se koncentrují údaje ze všech elektroměrů, plynůměrů, vodoměrů atd. a toto zařízení i ovládá blokování vybraných spotřebičů či sekcí (*regulační výstupy*).

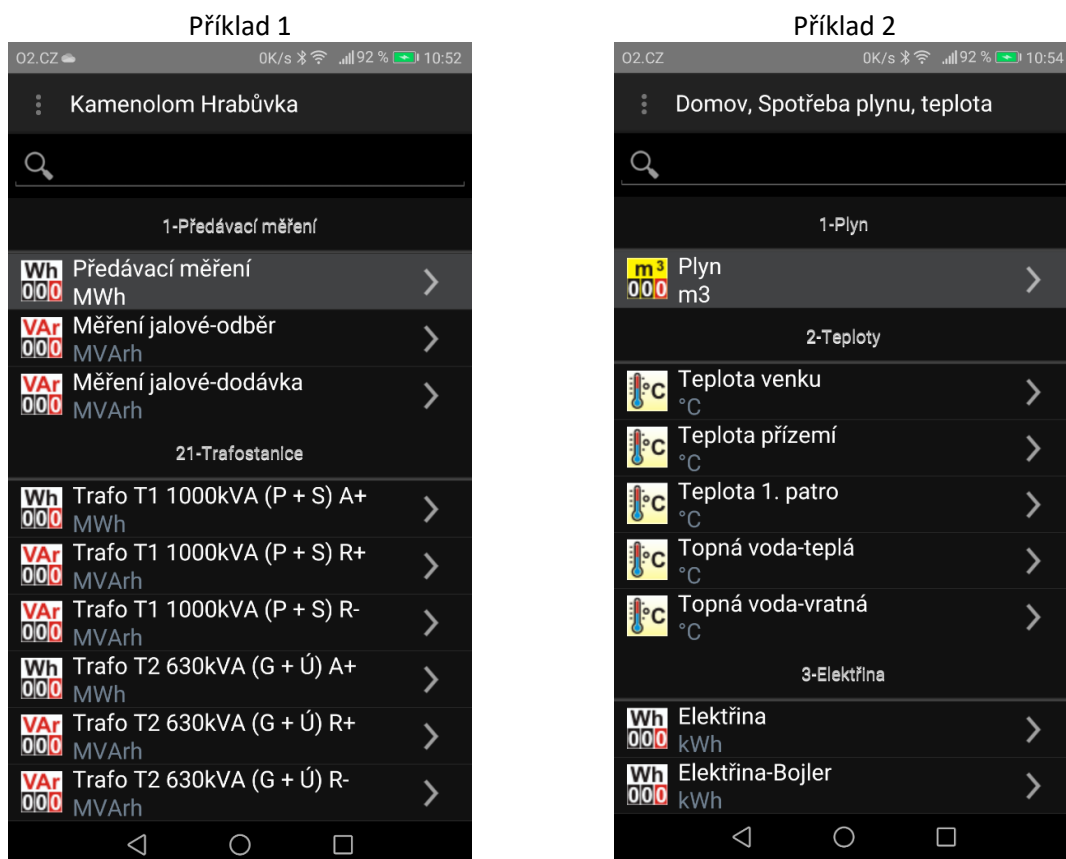
Vlevo nahoře je opět tlačítko pro menu, kde lze najít odkazy:

- **Uložená data** – odkaz na výpis měření vybraného projektu a následně uložená (offline) **data** tohoto **měření**.
- **Aktuální měření** – tímto se projekt na serveru MaxComm uvede do **stavu online**, tzn. server se připojí k zařízení pro měření a regulaci. Aplikace pak bude ze serveru dostávat aktuální hodnoty měření případně stav regulace na tomto provozu.
- **Info o projektu** – údaje o připojení, typu zařízení a stavu projektu



2.3 Výpis měření

Z okna výpisu projektů se na výpis měření dostanete kliknutím na tlačítko „Data“ nebo z menu „Uložená data“. Aplikace načte všechna definovaná měření vybraného projektu:



Ikona vlevo indikuje typ měření:

	Činný odběr nebo dodávka
	Jalový odběr nebo dodávka
	Plyn
	Teplo
	Voda
	Motohodiny
	Množství materiálu
	Teplota
	Vlhkost
	Účinník
	Napětí
	Proud
	Zkreslení napětí nebo proudu
	Stavové měření
	Obecné měření s agregací SUMA
	Obecné měření s agregací PRŮMĚR

Klepnutím na některé měření se aplikace přepne do režimu prohlížení uložených dat tohoto měření...

Prohlížeč uložených dat měření se liší dle typu měření:

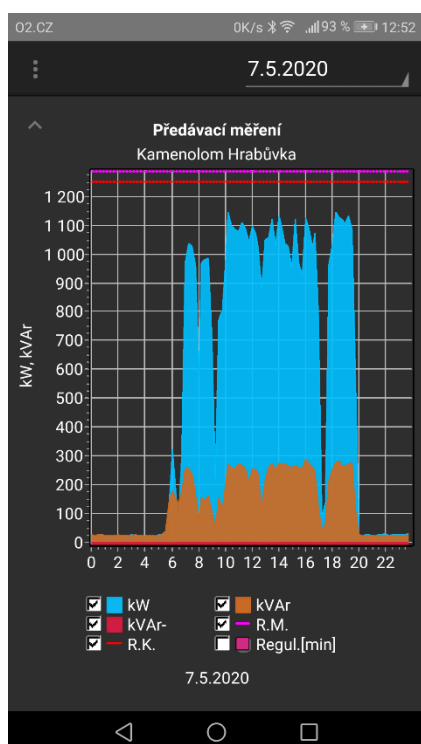
- Elektřina, předávací měření, odběr (*zobrazí se činné i jalové měření + regulační zásahy*)
- Elektřina, předávací měření, dodávka (*zobrazí se činné i jalové měření při dodávce*)
- Elektřina, podružné činné měření
- Elektřina, podružné jalové měření, odběr
- Elektřina, podružné jalové měření, dodávka
- Zemní plyn (*zobrazí se odběr od 6:00 do 6:00 následujícího dne*)
- Proud (*zobrazí se proud: špičkový, průměrný, max. zatížení a počet přetížení*)
- Napětí (*zobrazí se: min., max. a průměrné napětí a dále počet výpadků, podpětí a přepětí*)
- Obecné měření (*ostatní měření nezapadající do jiných skupin*)
- Odečet všech měření (*jen tabulka*)

2.4 Data měření

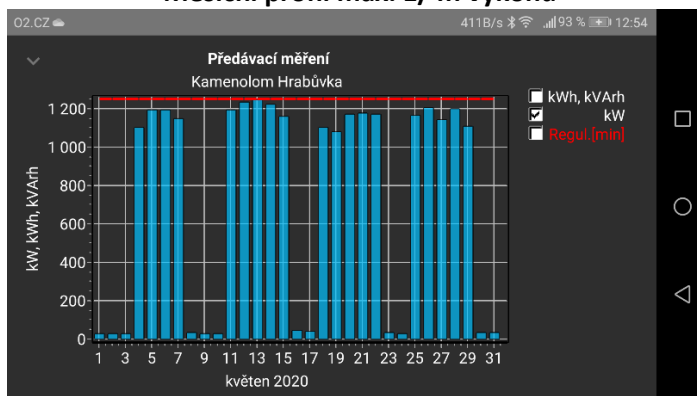
2.4.1 Elektřina, předávací měření, odběr

Pokud ve výpisu měření klepnete na měření patřící mezi „předávací“, zobrazí se sestava předávacího měření:

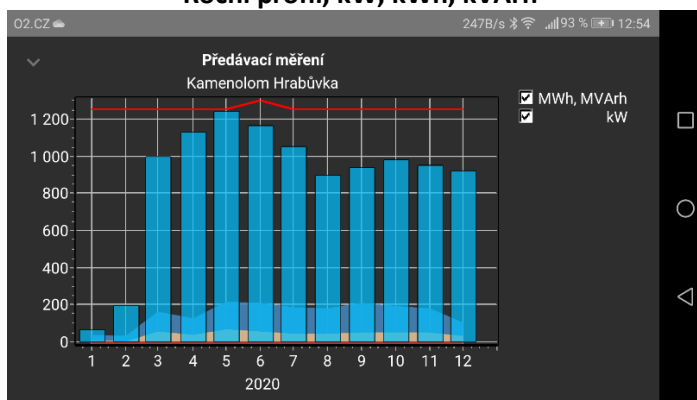
Denní profil výkonu, kW, kVAr



Měsíční profil max. 1/4h výkonu



Roční profil, kW, kWh, kVArh



Sestava předávacího měření:

- Činný odběr (dodávka), kW, kWh
- Jalový odběr a dodávka, kVAr, kVArh (při odběru nebo dodávce)
- Rezervovaná kapacita, kW (definováno v tabulce projektu)
- Regulované maximum, kW (s touto hodnotou pracuje regulátor)
- Počet regulačních zásahů

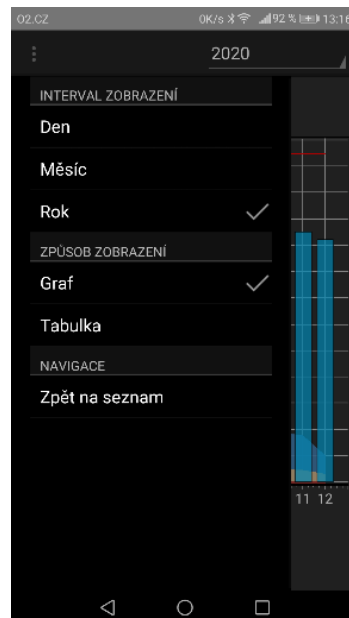
Aplikace reaguje na orientaci telefonu a zobrazení přizpůsobí tomu, zda je telefon položen **na šířku** nebo jej držíte normálně **na výšku**.

Přetažením prstu zleva doprava (v grafu) se načtou data z předchozího období.

Přetažením prstu zprava doleva (v grafu) se načtou data z následujícího období.

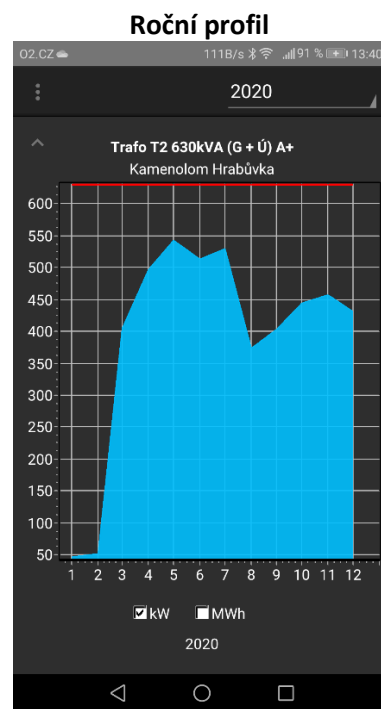
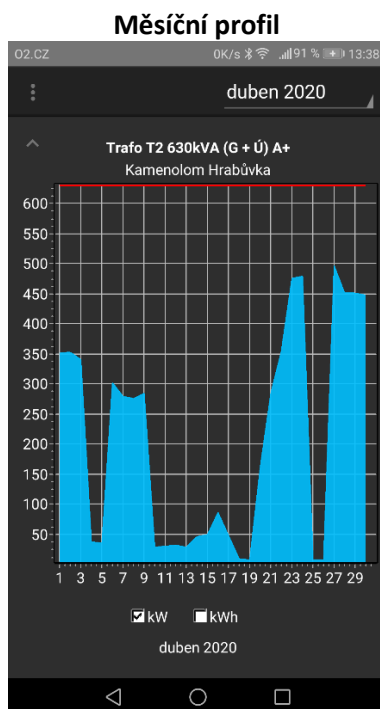
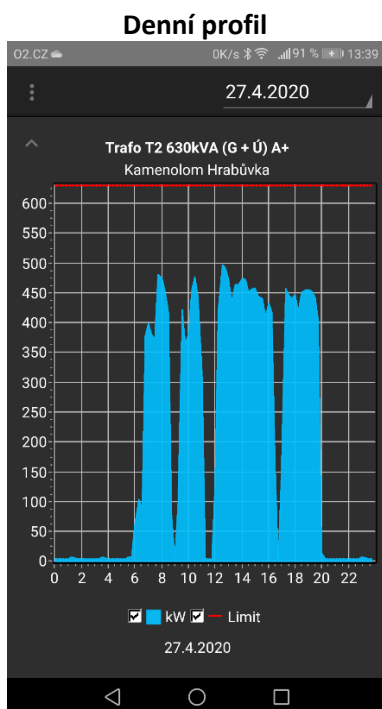
Jinak v kalendáři můžete rychle přejít na data zvoleného dne, měsíce či roku ...

Přepínání intervalu zobrazení (**Den – Měsíc - Rok**) a způsobu (**Graf - Tabulka**) najdete v menu...



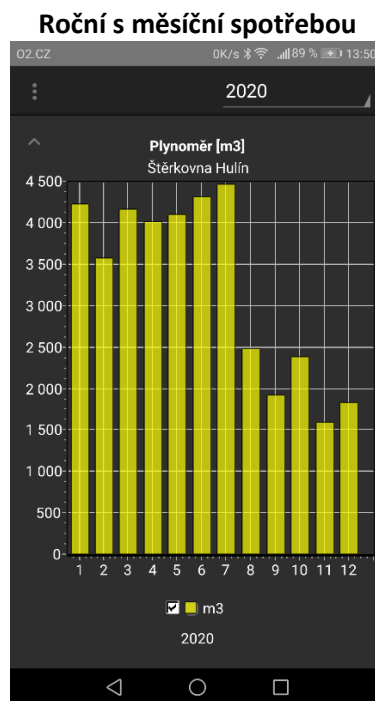
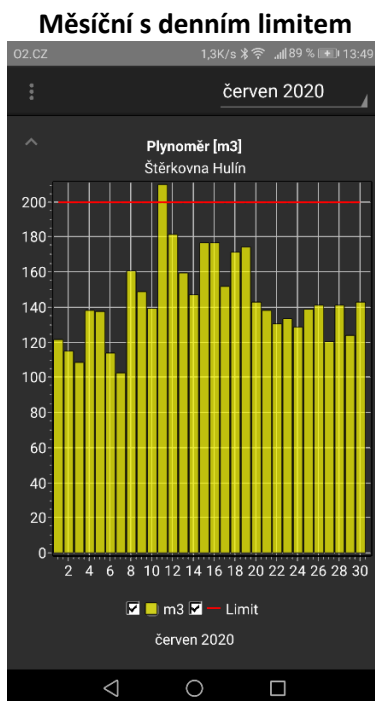
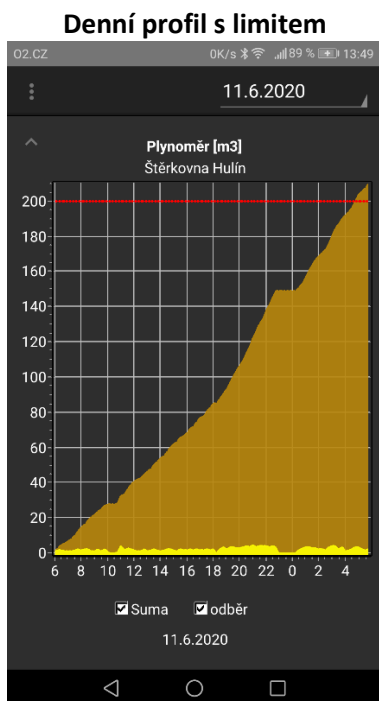
2.4.2 Elektřina, podružné měření

V měsíčním a ročním profilu lze zobrazit maximální naměřený 1/4h výkon v kW a také spotřebu v kWh, MWh.



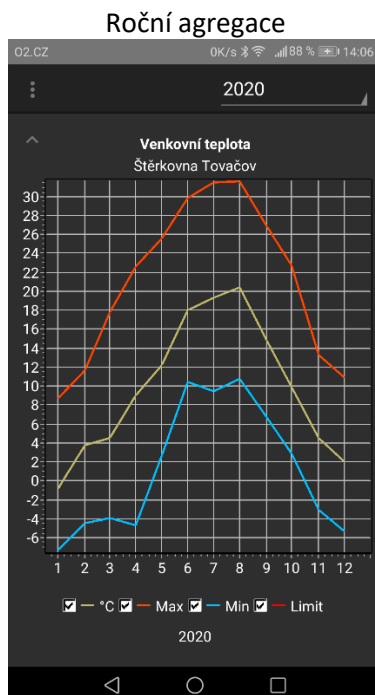
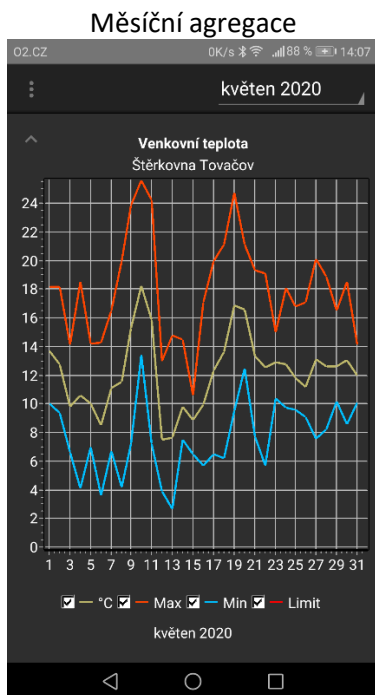
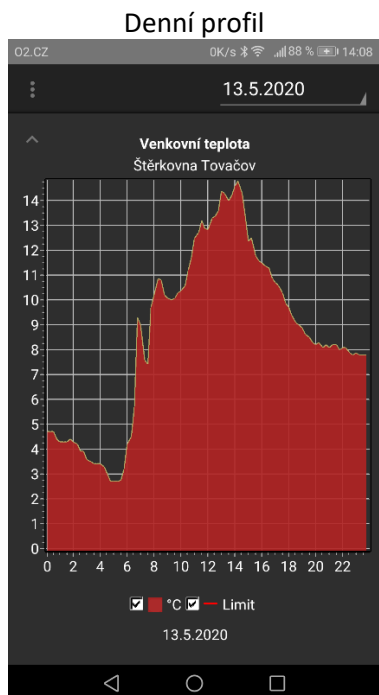
2.4.3 Zemní plyn

Vyhodnocení spotřeby zemního plynu je specifické v tom, že plynárenský den začíná v 6:00. To se týká i agregace denních a měsíčních hodnot.



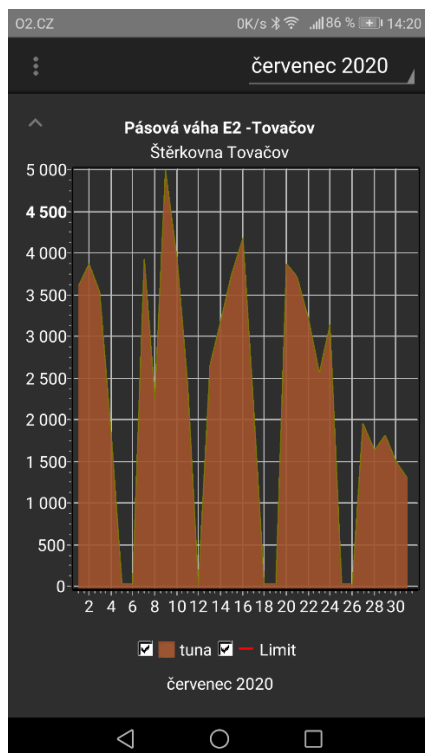
2.4.4 Měření teploty

Měření teploty je realizováno např. pomocí převodníků [TPC20](#) nebo [THPC-18](#), který měří současně i vlhkost.



2.4.5 Obecné měření, např. přeprava materiálu

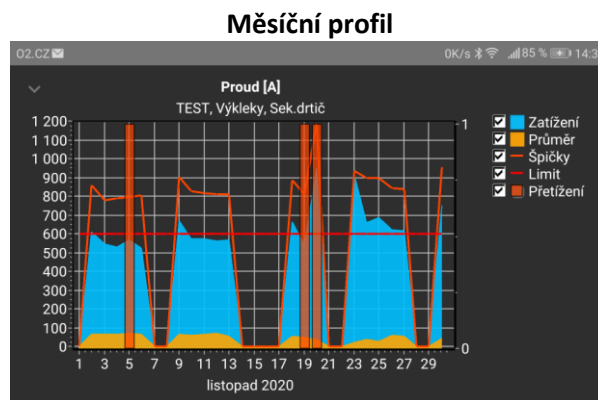
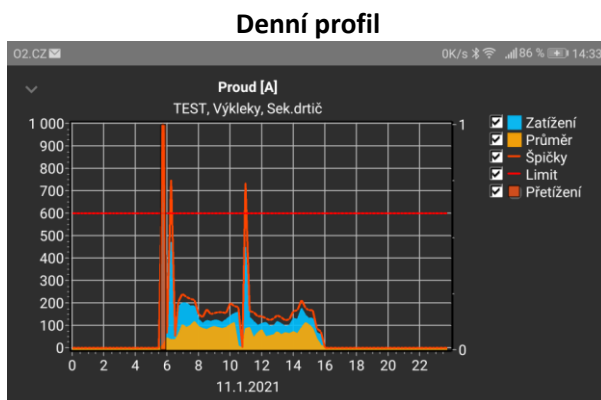
Na příkladu obecného měření je zde demonstrováno zobrazení dat v tabulce...



Pásová váha E2 -Tovačov, Štěrkovna Tovačov		
VII 2020	tuna	Limit
1.	3609	0
2.	3870	0
3.	3537	0
4.	1798	0
5.	28	0
6.	35	0
7.	3933	0
8.	2275	0
9.	5002	0
10.	3915	0
11.	2413	0
12.	33	0
13.	2669	0
14.	3190	0
15.	3728	0

2.4.6 Měření proudového zatížení

Měření proudového zatížení sítě a strojů je možné realizovat pomocí elektroměru [EME319](#).



Zatížení ... maximální hodnota tzv. „klouzavého“ průměru proudu. Tato hodnota by neměla překročit dimenzování jističe nebo pojistky. Časové okno pro výpočet klouzavého průměru by mělo být nastaveno dle charakteristiky jističe – viz návod k elektroměru [EME319...](#)

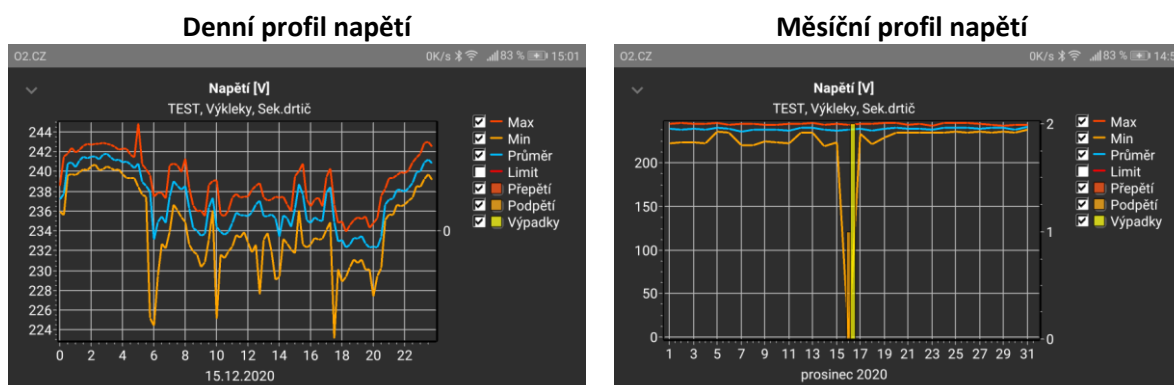
Špičky ... nejvyšší naměřený proud v intervalu 320 ms.

Průměr ... průměrný proud ve sledovaném období.

Přetížení ... počet přetížení ve sledovaném období (*vertikální osa vpravo*).

2.4.7 Analýza kvality napájecí sítě

Měření napětí v síti a zachycení událostí jako podpětí, přepětí či výpadků je možné realizovat pomocí elektroměru [EME319](#).



Min, Max, Průměr ... agregované hodnoty napětí v síti ve sledovaném období.

Přepětí, Podpětí, Výpadky ... počet těchto událostí (vertikální osa vpravo).

2.4.8 Odečet všech měření

Ve výpisu měření je v menu odkaz na data všech měření – tím se rozumí tabulka, kde jsou na řádcích všechna měření projektu a ve sloupci TOTAL je agregovaná hodnota za zvolený interval (Den – Měsíc - Rok).

červen 2020		
Přehled měření, Kamenolom Slapy		
VI 2020	TOTAL	Max
1-Předávací měření	---	---
Předávací měření	135 MWh	681 kW
Měření jalové-odběr	40,3 MVarh	263 kVAr
Měření jalové-dodávka	0 MVarh	0 kVAr
21-Trafostanice	---	---
Trafostanice-TS1-P+ 1000kVA	120 MWh	655 kW
Trafostanice-TS1-Q+ 1000kVA	0,613 MV...	5,52 kVAr

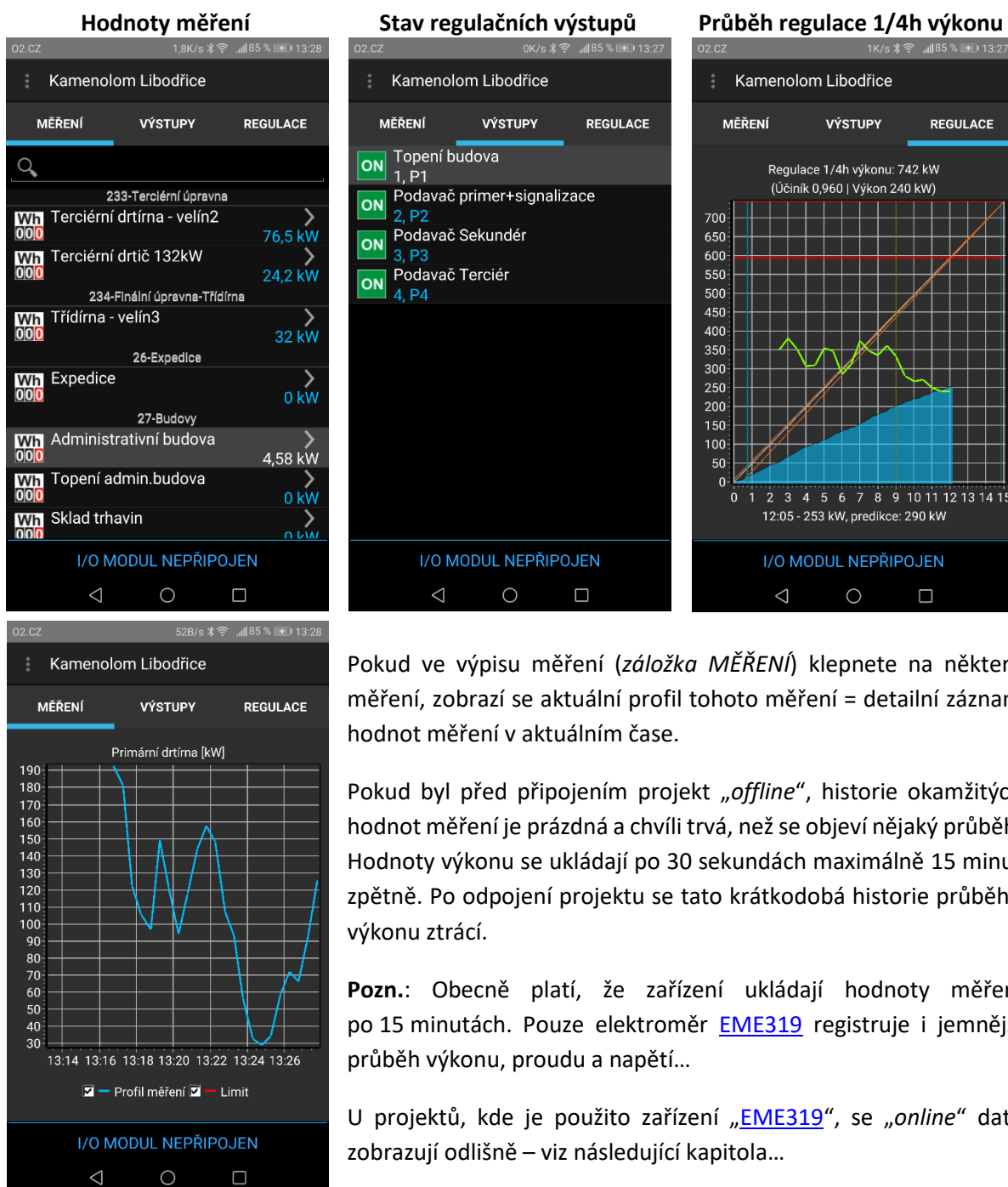
2.5 Aktuální hodnoty měření (online)

Ve výpisu projektů označte požadovanou položku (provozovnu) a klikněte na tlačítko:



Následně se aplikace přepne do režimu prohlížení online hodnot měření. Mezitím se server pokusí projekt uvést do stavu „online“. Tzn., že se server připojí k zařízení pro měření a regulaci, např.: regulátor [ATS-C120](#), elektroměr [EME319](#), měřicí modul [MM-116](#) a další...

Po úspěšném připojení začne server stahovat ze zařízení nová data od posledního spojení. To může trvat několik minut, ale i během stahování zařízení poskytuje aktuální údaje o stavu měření a regulace. Pokud je projekt již ve stavu „online“ (*připojil jiný uživatel*), nevadí, připojení k projektu je sdílené. Až se poslední uživatel od projektu odpojí, server uvede projekt do stavu „offline“.



Pokud ve výpisu měření (záložka **MĚŘENÍ**) klepnete na některé měření, zobrazí se aktuální profil tohoto měření = detailní záznam hodnot měření v aktuálním čase.

Pokud byl před připojením projekt „offline“, historie okamžitých hodnot měření je prázdná a chvíli trvá, než se objeví nějaký průběh. Hodnoty výkonu se ukládají po 30 sekundách maximálně 15 minut zpětně. Po odpojení projektu se tato krátkodobá historie průběhu výkonu ztrácí.

Pozn.: Obecně platí, že zařízení ukládají hodnoty měření po 15 minutách. Pouze elektroměr [EME319](#) registruje i jemnější průběh výkonu, proudu a napětí...

U projektů, kde je použito zařízení „[EME319](#)“, se „online“ data zobrazují odlišně – viz následující kapitola...

2.5.1 Aktuální hodnoty měření elektroměru EME319

V předchozí kapitole se nachází vizualizace „online“ dat obecných zařízení pro měření a regulaci 1/4h výkonu nebo denní regulace spotřeby zemního plynu. Elektroměr [EME319](#) poskytuje specifická data, proto má i samostatný formulář pro prezentaci aktuálních hodnot měření.

„Online“ hodnoty měření elektroměru [EME319](#) jsou rozděleny do tří skupin:

- **Aktuální měření** – aktuální hodnoty výkonů, účinníku, napětí, proudů a THD
- **Stav číselníků** – aktuální stav registrů činné a jalové energie
- **Extrémní hodnoty** – nejvyšší naměřené hodnoty a počítadla přetížení, výpadků, přepětí, ...



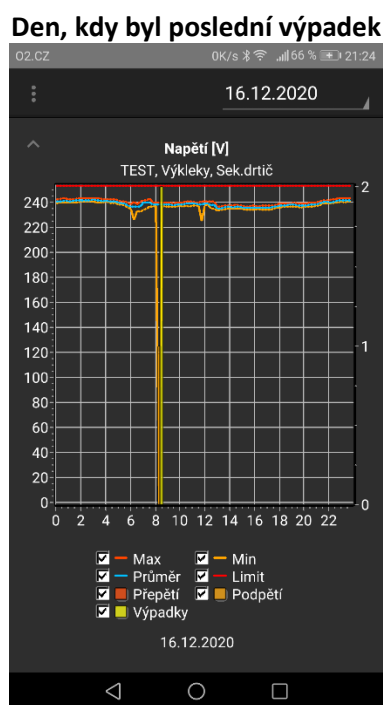
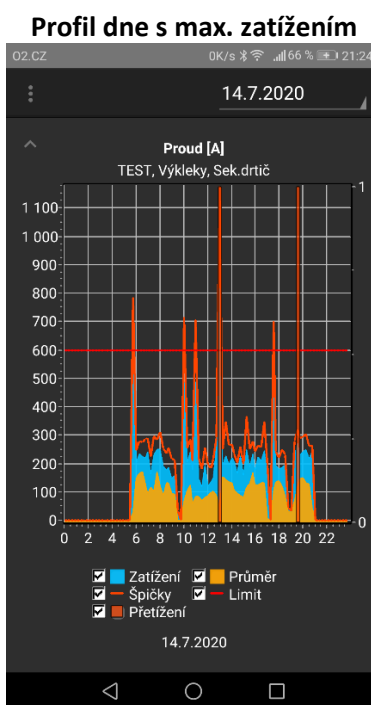
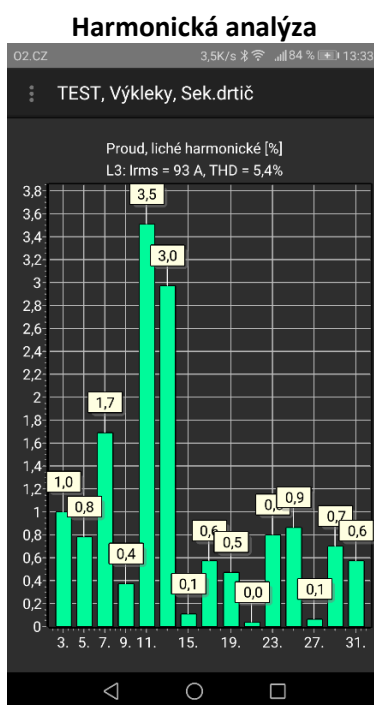
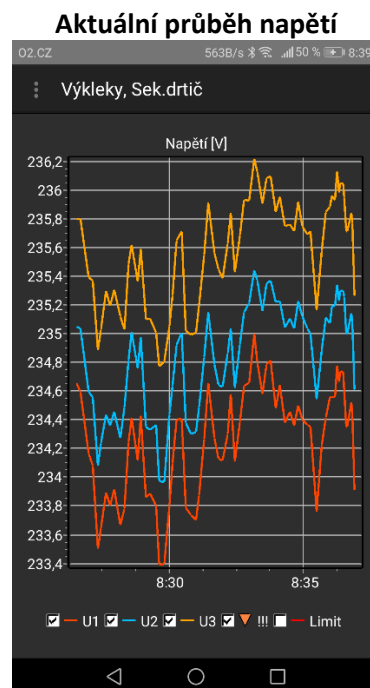
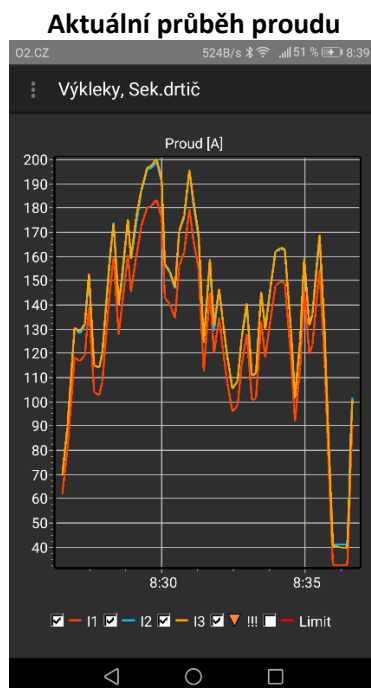
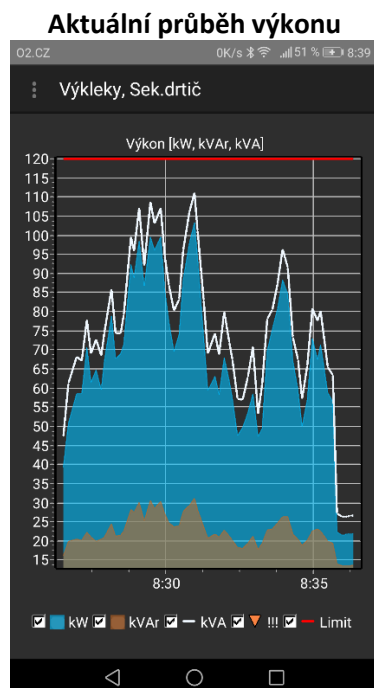
...a ještě další údaje následují...

Také zde platí, že poklepáním na některý řádek se zobrazí časový profil průběhu hodnot zvoleného měření – viz následující stránka. Podobně jako u obecného zařízení i pro elektroměr server uchovává historii posledních naměřených hodnot jen pokud je projekt ve stavu „online“.

Pozn.: Elektroměr EME319 kromě ¼h hodnot ukládá do paměti i detailní průběh měření, tento se zde ale nezobrazuje. K prohlížení této detailní paměti není mobilní aplikace vhodná, a proto zde tato funkce není implementována. Pro tyto účely použijte desktopovou aplikaci [Max Communicator](#) nebo speciální program [EMEX](#) určený přímo pro elektroměry EME319...

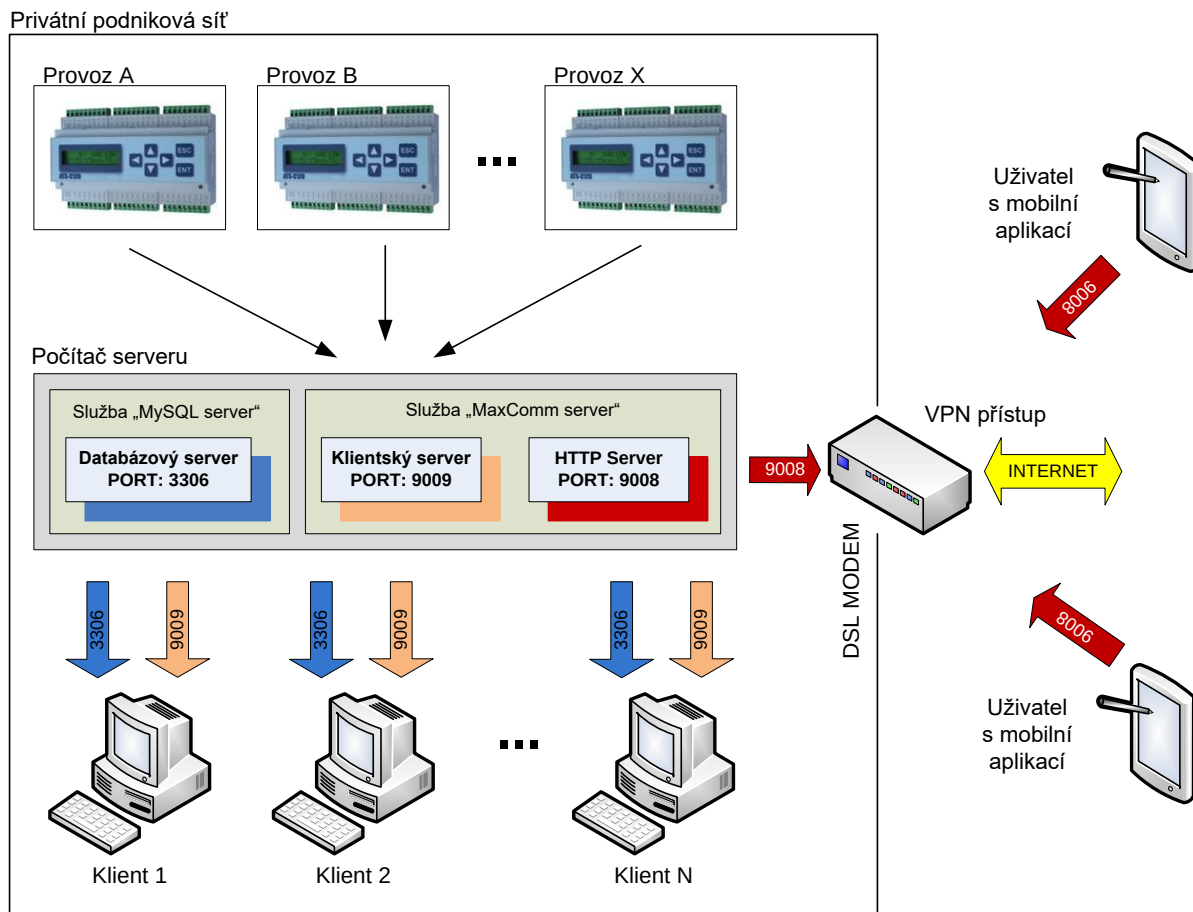
Poklepem na měření ve skupině „Stav číselníků“ nebo „Extrémní hodnoty“ se místo aktuálního profilu měření zobrazí naopak „offline“ uložená data – profil „inkriminovaného“ dne. Např. poklepem na řádek „Špičk. proud“ se zobrazí **denní profil proudu ze dne, kdy byl naměřen nejvyšší špičkový proud**...

Ukázky časového průběhu měření elektroměru [EME319](#) u některých vybraných veličin („online“ i „offline“ data)...



3 Topologie a bezpečnost systému

Na obrázku níže je znázorněna struktura komunikace mezi všemi prvky systému:



Legenda:

- **Provoz X** ... jedna provozovna s celým systémem měření a regulace = elektroměry, komunikační moduly, hlavní řídicí jednotka, moduly relé pro blokování spotřebičů atd.
- **Počítač serveru** ... nutně nemusí jít o speciální server, stačí běžná pracovní stanice s trvalým provozem.
 - **Databázový server** ... MySQL verze 8
 - **Klientský server MaxComm** ... TCP/IP server pro připojení místních klientů přes desktop aplikaci
 - **HTTP server** ... je součástí služby MaxComm serveru. Využívá technologii komunikace REST/API na protokolu HTTP. Tento server je určen jen pro komunikaci s mobilními klienty.
- **Klient N** ... uživatel systému, který se pomocí své desktopové aplikace programu Max Communicator připojuje na „MaxComm server“ a „Databázový server“. Nepoužívá HTTP server. **Tito klienti se připojují v rámci privátní podnikové sítě!**
- **DSL modem** ... přístupový bod k internetu. Nemusí jít nutně právě o DSL modem. Internetová přípojka může být realizována různými způsoby. Tento přístupový bod je třeba ale nakonfigurovat tak, aby se bylo možné bezpečně z internetu připojit na HTTP server pomocí zde popisované mobilní aplikace...

- **Uživatel s mobilní aplikací** ... oprávněný uživatel s mobilním telefonem s internetovým připojením a nainstalovanou aplikací **Max Communicator**. Tito klienti se připojují z veřejné sítě internet na **HTTP server**. Nemají přímý přístup na klientský ani databázový server! Všechny požadované údaje a pokyny poskytuje a zprostředkovává **HTTP server**.

3.1 Zabezpečení systému proti neoprávněnému přístupu

Jakýkoli vstupní bod z veřejné sítě internet do privátní podnikové sítě je nutné kvalitně zabezpečit proti vniknutí neoprávněným subjektům!

3.1.1 Zabezpečení na úrovni aplikace

První linií zabezpečení je samotné aplikační rozhraní. Již při návrhu této mobilní aplikace byla bezpečnosti věnovaná maximální priorita:

- **Z mobilní aplikace není možné provádět jakékoli změny** ani v databázi ani nastavovat zařízení, nelze ovládat regulační výstupy nebo dokonce přistupovat k prostředkům počítače serveru! **HTTP server MaxComm** má striktně naprogramován jen omezený soubor **REST/API funkcí** a nic navíc prostě vykonat ani neumí.
- **Přístup k REST/API rozhraní HTTP serveru je podmíněn přihlášením uživatele!**
- Komunikace mezi aplikací a HTTP serverem sice probíhá otevřeným protokolem HTTP, ale **přihlášení a průběžná komunikace je zabezpečena šifrovanými klíči** (*autorizace DIGEST*). Heslo nelze tedy odposlechnout ani opakovat zachycené požadavky. Navíc v případě použití **VPN přístupu** (*doporučeno, viz dále..*) je **komunikace šifrována i bez protokolu HTTPS**.

3.1.2 Zabezpečení přístupového bodu

Přístupovým bodem se rozumí zařízení, které propojuje veřejnou síť internet s privátní podnikovou sítí. Počítače uvnitř obvykle komunikují směrem ven do internetu nebo uvnitř mezi sebou v rámci lokální uzavřené sítě.

Přístup z veřejné sítě do vnitřní sítě (*což z této aplikace potřebujeme*) není bez určitých opatření možný. Některé postupy, jak toho dosáhnout, budou podrobněji nastíněny v kapitole „*Instalace*“. Jedním z hlavních hledisek při výběru technického řešení by měla být dostatečná úroveň zabezpečení a zvážení možných rizik – zda při zvoleném řešení hrozí či ne, případně je dodatečně ošetřit dalšími opatřeními.

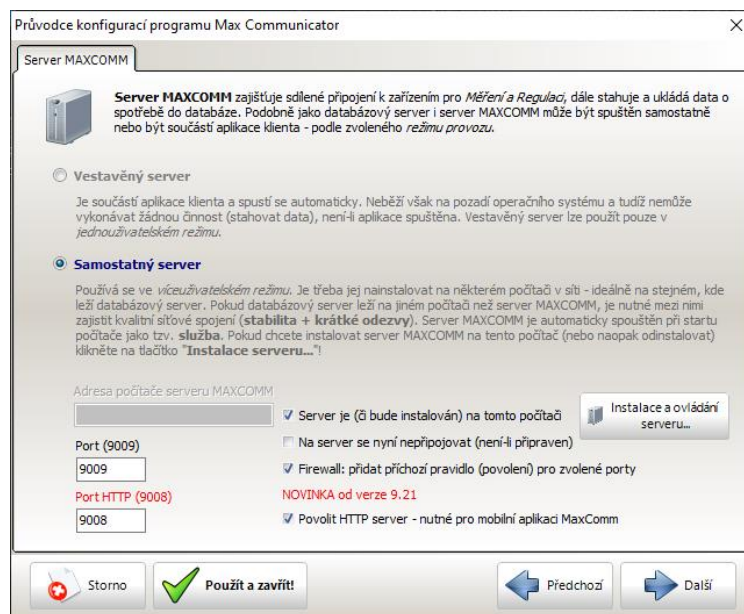
Tyto **vstupní body do sítě** jsou první na „ráně“ a potenciálnímu útočníku obvykle i přístupné – pokud se jedná např. o veřejnou službu (*není náš případ*). A proto je jejich zabezpečení věnována taková pozornost, že potenciální útočník obvykle volí snazší přístup – např. formou zavírovaného emailu...

V případě této aplikace je výhodou, že okruh uživatelů systému je omezený a je dopředu znám. Lze tedy použít velmi účinné prostředky zabezpečení typu omezení přístupu jen ze známých adres nebo zařízení a samozřejmě nejlépe pomocí vlastní **Virtuální Privátní Sítě**, která zajistí soukromé připojení i z veřejného internetu...

4 Instalace

4.1 Příprava serveru MaxComm

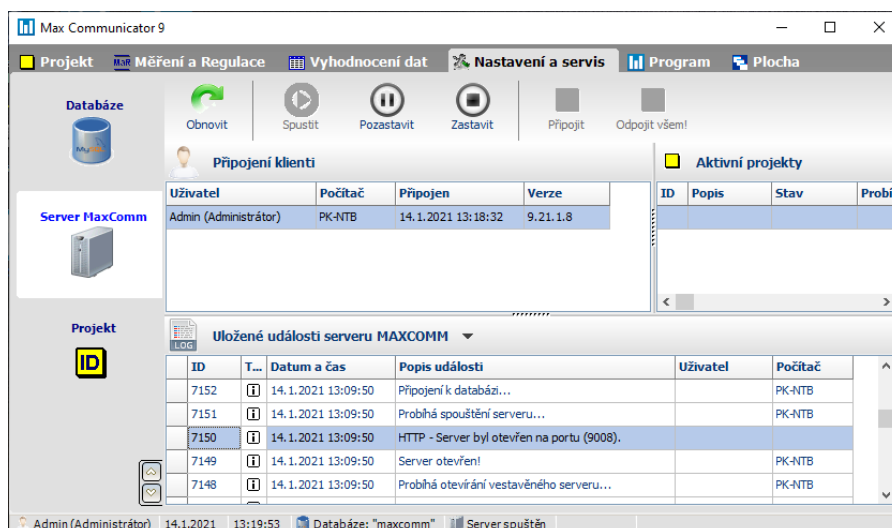
Konfigurace serveru MaxComm pro použití mobilní aplikace je velmi jednoduchá – stačí v konfiguraci programu **povolit HTTP server** na portu **9008** (nebo zadat jiný port) a přidat výjimku do Firewallu pro tento port:



Poznámky:

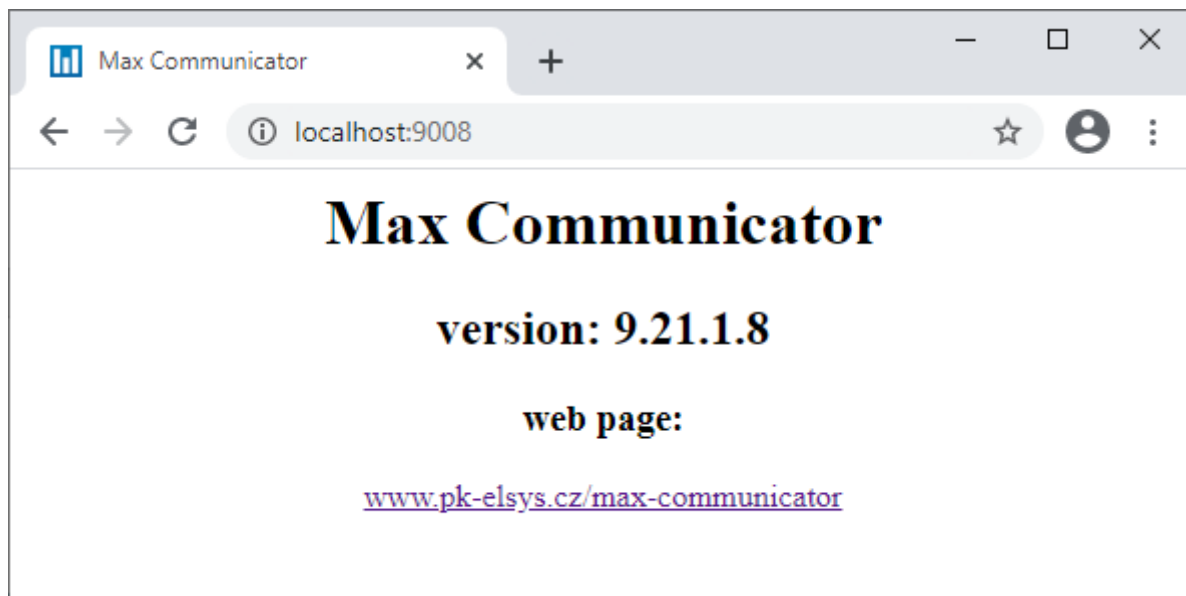
- Je třeba mít aktuální verzi programu (*minimálně 9.21*)!
- Je třeba použít klient-server (*víceuživatelský*) režim provozu se samostatným serverem MaxComm a serverem MySQL!
- **Nezapomeňte všem uživatelským účtům přiřadit hesla!**
- **Nezapomeňte na počítači serveru nastavit statickou IP adresu!**

Po restartu aplikace si ověřte, že se HTTP server opravdu otevřel – na záložce „Nastavení a servis – Server MaxComm“:



Dále je dobré ze stejného a potom z jiného počítače ověřit, že port HTTP serveru je opravdu dostupný, a to pomocí běžného internetového prohlížeče:

Test HTTP serveru na stejném počítači (zadejte adresu: „<http://localhost:9008>“):



Test HTTP serveru z jiného počítače nebo mobilu připojeného na místní WIFI
(tímto se ověří, že firewall neblokuje HTTP port)

02.CZ

0K/s 37 % 13:34

192.168.1.8:9008

Max Communicator

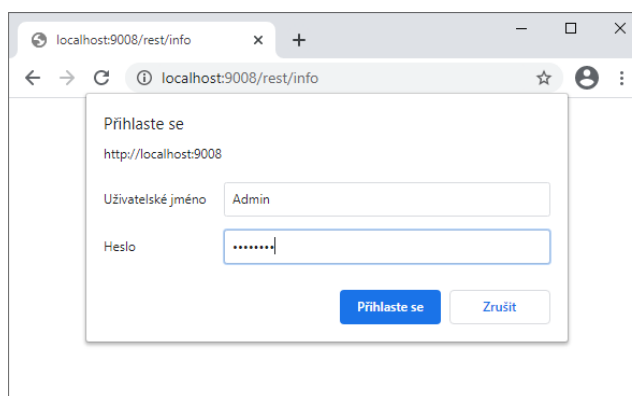
version: 9.21.1.8

web page:

www.pk-elsys.cz/max-communicator

HTTP server aktuálně nemá žádnou webovou aplikaci (*možná v budoucnu*) a kromě úvodní hlavní stránky zde mimo REST/API již dál nic není.

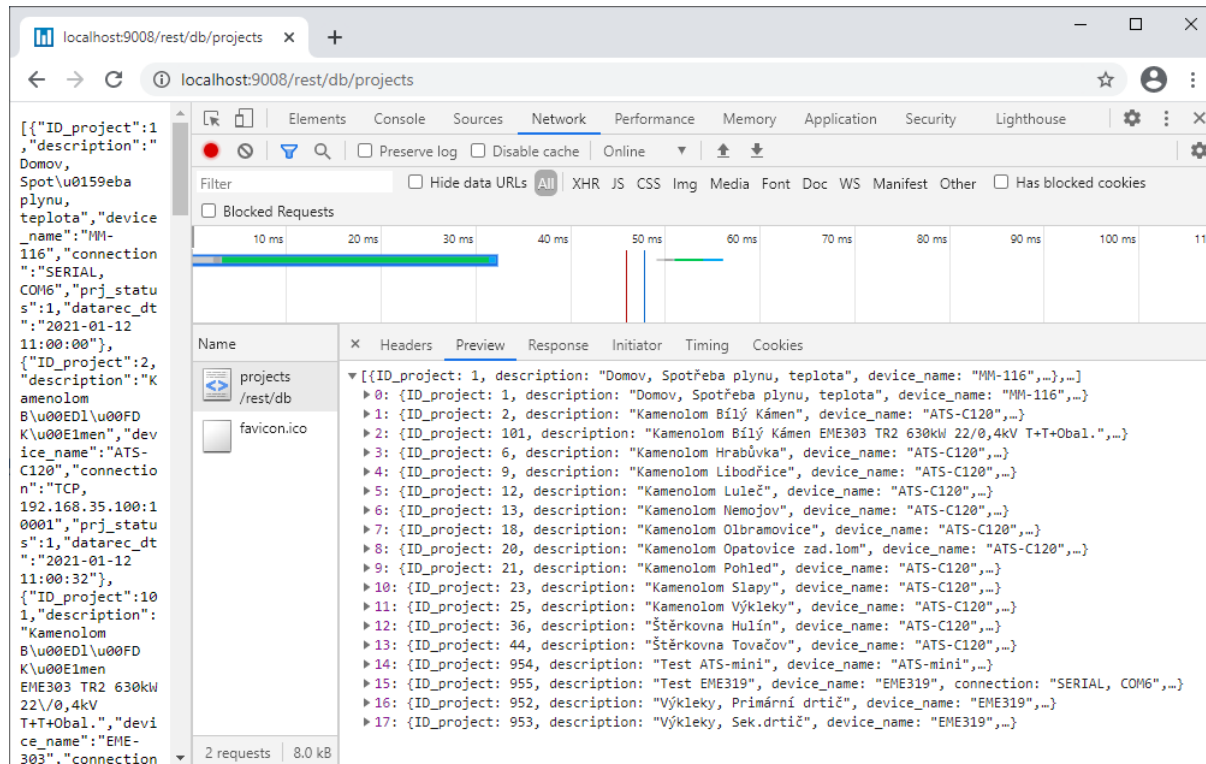
Přístup k REST/API lze přes webový prohlížeč ověřit také, ale už bude vyžadováno přihlášení uživatele:



Odpověď HTTP serveru:



Seznam projektů:



...atd. Takto aplikace vyčítá data z HTTP serveru...

4.2 Konfigurace přístupového bodu

Toto je úkol pro IT oddělení, aby v první řadě tuto aplikaci schválilo z hlediska bezpečnosti a poté zajistilo zabezpečený přístup z veřejné sítě k HTTP serveru programu Max Communicator. U větších nadnárodních firem to bude možná trochu náročnější proces...

Postup, který je dále nastíněn vám však může pomoci se s problematikou alespoň trochu seznámit, případně nasměrovat na kompetentní lidi. Pro menší firmy s jednoduchou sítí a trochu zdatnější IT laiky by však tento návod mohl i stačit. Technicky to až tak moc složité není.

Nejsem specialista na sítě, a tak pokud někdo v následujícím postupu najde nějaké slabiny nebo zná nějaká další šikovná řešení, budu rád za zpětnou vazbu (info@pk-elsys.cz)... A teď, jdeme na to!

V první řadě je třeba **ve firmě zajistit internetové připojení s veřejnou statickou IP adresou**! Běžné internetové připojení používá tzv. „*dynamickou IP adresu*“, což stačí na prohlížení obsahu internetu, ale zpětný přístup z internetu (což *potřebujeme*) už možný není. Existují i varianty přístupu přes zprostředkovatele, ale tudy raději nepůjdeme... Příplatek za pevnou IP adresu je totiž „jen“ asi 100,- Kč/měsíc, což by pro firmu neměl být problém...

Takže nyní máme pevnou IP adresu, která je viditelná po celém světě a co dál? Nabízím dvě varianty:

- **Předávaný port** – jednoduché na konfiguraci, doporučuji vyzkoušet jako první možnost a až bude vše fungovat, přejít na bezpečnější VPN...
- **Připojení VPN** – šifrované připojení pomocí VPN tunelu (**DOPORUČENO**).

4.2.1 Varianta komunikace pomocí „předávaného“ portu

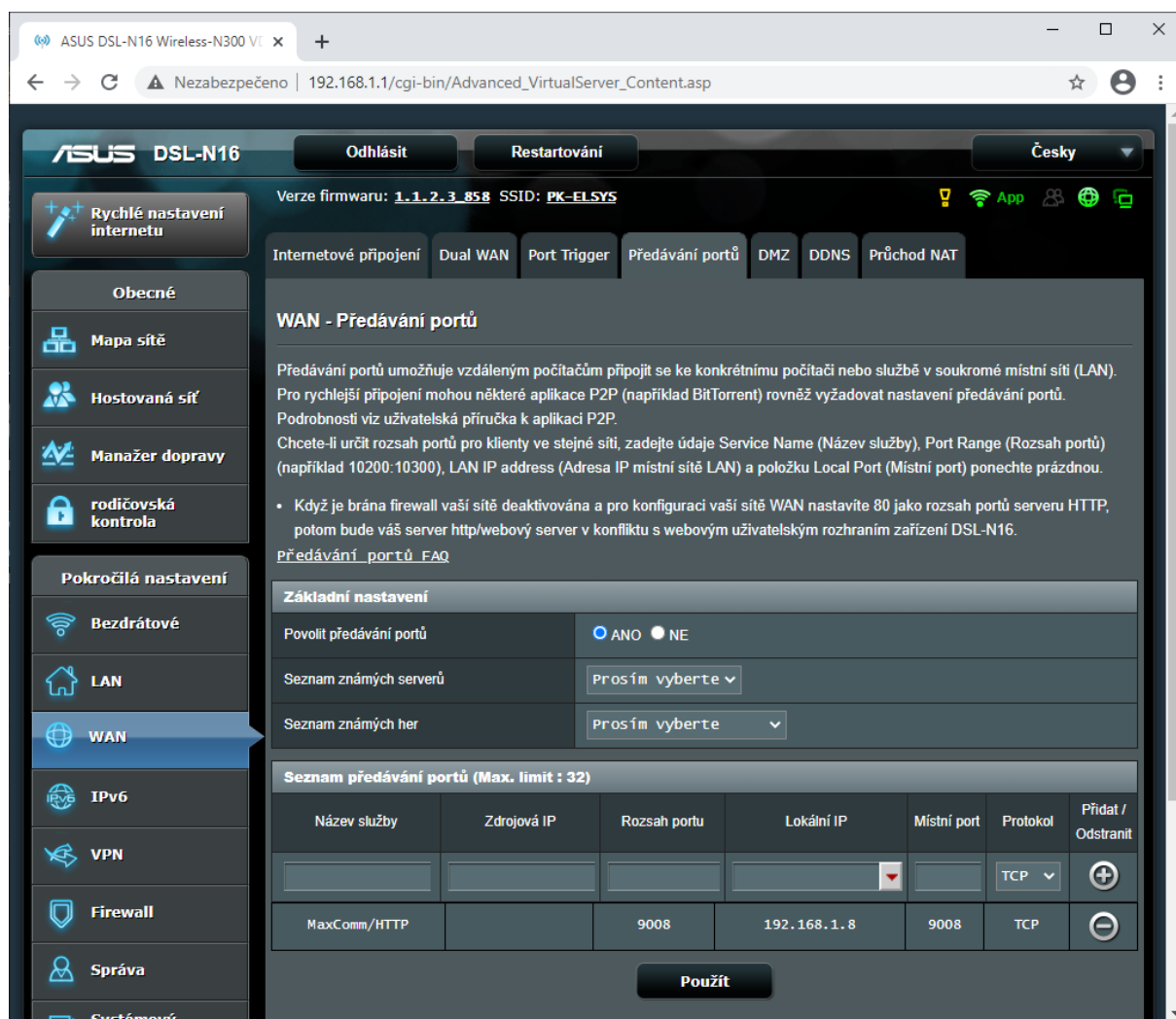
Komunikace v sítích TCP/IP funguje přes tzv. „porty“. Na jedné IP adrese (*počítač*) může být otevřeno několik těchto portů a k nim propojeny rozličné služby. Není-li otevřen žádný port, nikdo se nemůže na nic připojit (*zjednodušeně řečeno*).

Takže, náš přípojný bod (*např. modem DSL*) má veřejnou IP adresu a nyní potřebujeme zpřístupnit nějaký port, na který navážeme požadovaný HTTP server! Pro tyto účely na routerech existuje služba „*Předávání (přesměrování) portů / Port forwarding*“. Pokud nějaká aplikace otevře z venku tento port, router přesměruje tento požadavek na cílové zařízení v lokální síti (*naš HTTP server*) a je to! Takže opravdu nic složitého.

Nevýhody tohoto řešení – IP adresa je veřejná a viditelná odkudkoli, třeba z Číny nebo Ruska a port je otevřený rovněž pro kohokoli. Existují „*programy-roboti*“, kteří skenují síť a hledají a hledají, až něco najdou... I když je rozhraní REST/API HTTP serveru programu MaxComm bezpečné, a i v případě uhádnutí hesla tam není co poškodit, nejde nic změnit, nelze ani šmírovat citlivá osobní a firemní data (*pomím data o spotřebě*), je to přinejmenším „*nepříjemné*“. Někdy vtípálek může např. zkoušet, co náš server vydrží častými opakovanými i když třeba neúspěšnými dotazy...

Tudíž tohle řešení je skvělé pro svou jednoduchost, určitě bych ho nezavrhoval, ale je třeba vědět, že připojení je veřejné a sem tam ten port někdo na zkoušku otevře. Sice se dál nedostane, ale pokud zjistíme nějaké podezřelé chování – jako časté opakované pokusy o přihlášení z exotických adres, bude lepší přejít na síť VPN...

Nyní praktická ukázka nastavení DSL routeru pro předávání portů. Do webového prohlížeče vložte adresu vašeho routeru, přihlaste se a najděte službu „Předávání portů / Port Forwarding“:



V mém případě leží HTTP server na počítači s adresou: 192.168.1.8. Vstupní i cílový port je nastaven stejně: 9008. Teoreticky se porty mohou lišit, ale zde pro to není důvod. To má smysl, pokud se překrývají dvě stejné služby.

Pozor, v mobilní aplikaci se nebude v nastavení připojení na HTTP server vkládat jeho lokální adresa (zde 192.168.1.8), ale veřejná statická IP adresa vašeho připojení!

Tip 1: Jakou internetovou adresu vlastně mám? Na internetu najdete řadu služeb, které vaši adresu zobrazí. Do vyhledávače zadejte třeba: „my ip“.

Tip 2: Jak zjistit adresu routeru v síti? Spustit příkazový řádek: (**Win+R**), zadat **CMD** a spustit. Pak zadat: **IPCONFIG** a potvrdit klávesou „Enter“. Hodnota „Default Gateway“ nám prozradí, kde hledat hlavní router... Tuto adresu pak vložte do internetového prohlížeče a přihlaste se do správy routeru. Dál už je třeba postupovat dle typu zařízení.

Tip 3: Pokud máte nějaký starší typ routeru, raději kupte nový!

4.2.2 Varianta komunikace pomocí VPN

Nevýhody otevřené komunikace mobilním zařízením do privátní firemní sítě přes veřejnou síť internet (např. WIFI v kavárně, ...) jsou i pro laika zřejmé. Bezpečnější je veškerou komunikaci vést šifrovaně, a navíc skrýt soukromé firemní prostředky (počítače) pro všechny nezvané návštěvníky. A k tomu právě slouží síť VPN. Nikdo, kdo ve svém zařízení (počítač, telefon, tablet, ...) nemá odpovídajícího VPN klienta s platnými autorizačními údaji, se k těmto privátním zdrojům informací nemůže vůbec dostat a ani odposlechnout komunikaci!

Konfigurace vlastní sítě VPN vyžaduje několik kroků na straně vašeho routeru (VPN server), ale i telefonu (VPN klient). Předem je třeba říci, že existuje mnoho způsobů a výrobců, jak realizovat síť VPN. Pokud to budete řešit sami bez pomoci IT oddělení, je vhodné vycházet z možností vašeho routeru a samozřejmě telefonu. Pokud máte něco staršího (více jak 8 let), raději poříďte nový router – vyplatí se to, ať nemarníte čas experimentováním...

Já zvolil variantu **OpenVPN**:

The screenshot shows the ASUS DSL-N16 web interface for configuring the VPN server. The browser address bar shows the URL 192.168.1.1/Advanced_VPN_OpenVPN.asp. The interface is in Czech and displays the 'Server VPN - OpenVPN' configuration page. The 'Povolit Server OpenVPN' (Enable Server OpenVPN) toggle is turned ON. The 'Port serveru' (Server port) is set to 1194. The 'RSA Encryption' is set to 1024 bit. The 'Client will use VPN to access' option is set to 'Internet and local network'. The 'Exportovat konfigurační soubor protokolu OpenVPN' (Export OpenVPN protocol configuration file) button is visible. Below the settings, there is a section for 'Uživatelské jméno a heslo' (Username and password) with a table listing users: 'admin' and 'petr'. The 'petr' user is currently connected, indicated by a green status and a red highlight on the password field.

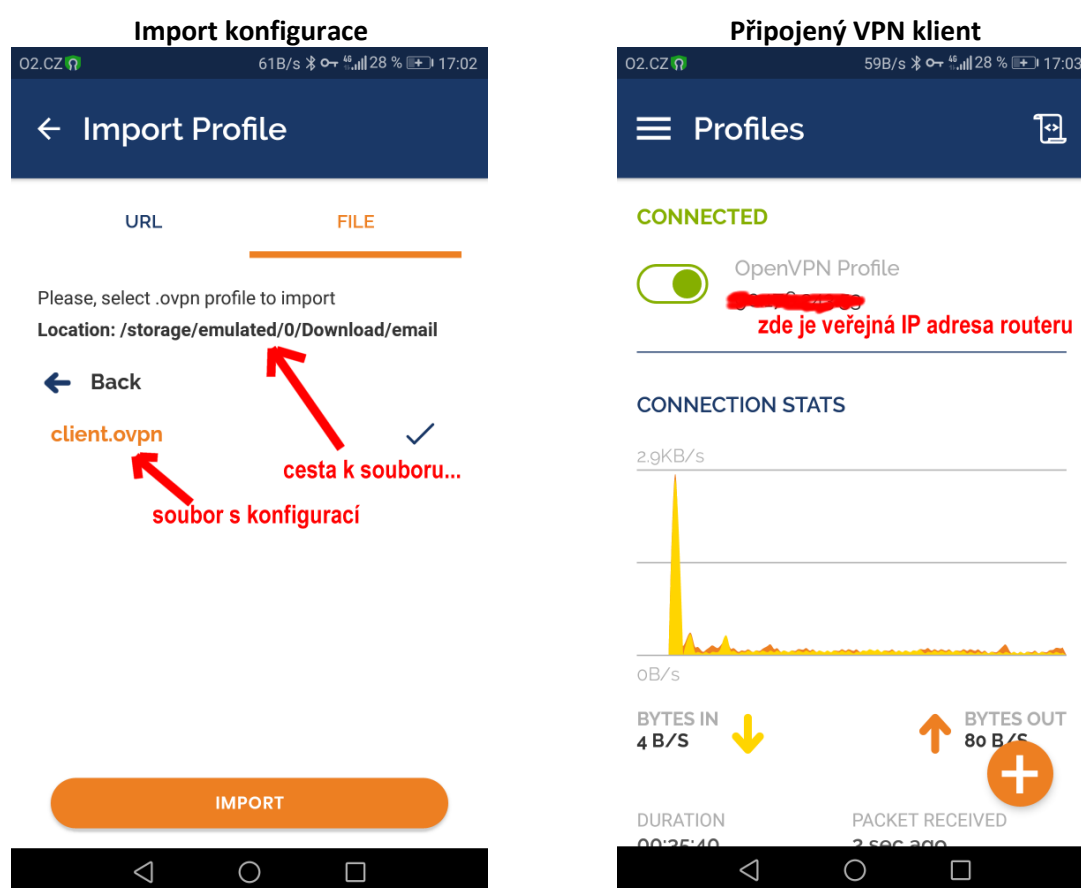
Stav připojení	Vytočit číslo	Heslo	Přidat / Odstranit
-			+
Odpojeno	admin	-	-
Připojeno	petr		-

Nejdříve je třeba povolit **OpenVPN** server a přidat uživatelské účty – zvolte silná hesla! Pak klikněte na tlačítko „Exportovat“. Router vygeneruje konfigurační soubor: „client.ovpn“, který budete potřebovat v telefonu při konfiguraci klienta. Tento soubor přeneste do telefonu, pokud možno bezpečnou cestou např. přes soukromý cloud nebo budiž, pošlete v příloze emailu:).

Pozn.: Ještě je dobré rozhodnout, zda povolit nebo zakázat přístup z telefonu na internet během doby, kdy je aktivní VPN připojení (*Local network only / Internet and local network*). Lze tam konfigurovat i řadu dalších parametrů v rozšířeném zobrazení (*např IP adresa telefonu při aktivním VPN*). Já nechal default hodnoty.

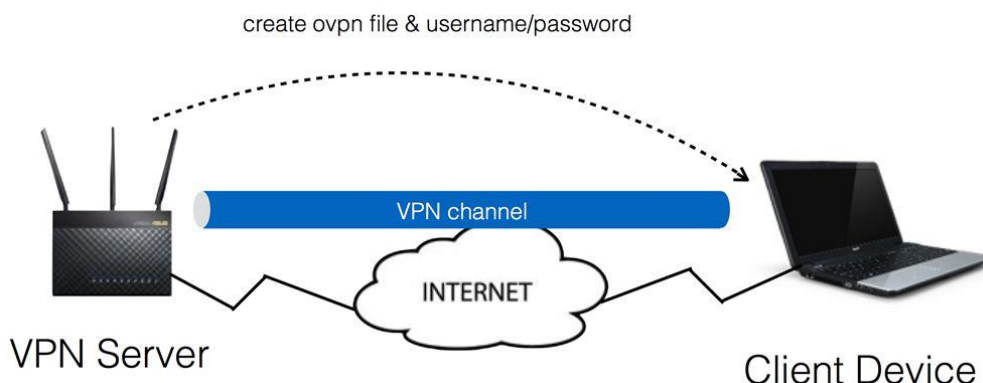
Dále už se pokračuje na telefonu. Je třeba říci, že telefony mají v sobě již nějaké možnosti VPN připojení zabudované – podívejte se do nastavení telefonu... Můj 5 let starý Huawei taky má nějakého VPN klienta, ale ne zrovna **OpenVPN**. Takže jsem **OpenVPN** klienta stáhnul z Google Play Store (*platí pro telefony s OS Android*)...

Po spuštění aplikace klienta **OpenVPN** na mobilním telefonu je třeba do něj vložit již připravený konfigurační soubor: „client.ovpn“ vygenerovaný routerem (*použil jsem přenos souboru přes email a pak přílohu v telefonu uložil do složky „download“*):



Důležitá poznámka: V aplikaci **Max Communicator** při konfiguraci připojení serveru zadejte do políčka „Adresa serveru“ hodnotu **lokální IP adresy HTTP serveru** (v mém případě: 192.168.1.8)! To je rozdíl proti variantě „Předávání portu“, kde se zadává **veřejná IP adresa**! V případě **VPN přístupu** má totiž mobilní telefon **přístup přímo do privátní firemní sítě** jako by byl připojen třebaš přes místní WIFI!

Před spuštěním aplikace **Max Communicator** je třeba na telefonu samozřejmě spustit aplikaci **OpenVPN** (nebo jiný) a připojit se do VPN sítě. Po ukončení práce s aplikací **Max Communicator** klienta VPN zase odpojte.



Na rozdíl od „port-forwarding“ varianty je použití sítě VPN o něco méně pohodlné, ale za to bezpečnější a má to řadu dalších benefitů – jedinou službou lze bez dalších opatření získat plnohodnotný přístup k prostředkům firemní sítě (v podstatě práce jako v lokální síti).

4.3 Instalace a konfigurace aplikace na telefonu

Pozn. 1: V době vydání této pracovní verze návodu (leden 2021), který je určený nejdříve pro odborníky a servis-many, je aplikace „**Max Communicator**“ dostupná pouze „interním testerům“. Chcete-li se zúčastnit testování aplikace, přihlaste se na email: info@pk-elsys.cz.

Pozn. 2: Z toho je zřejmé, že aplikace bude nejdříve dostupná pro telefony s OS „**Android**“.

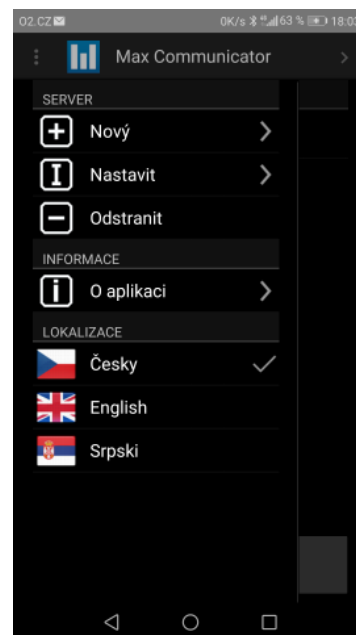
Pozn. 3: Telefony „**iPhone**“ s „**iOS**“ budou řešeny možná později.

Pozn. 4: Operační systém „**Android**“ umožňuje stahovat aplikace z více oficiálních obchodů, ale také i z neoficiálních zdrojů, tzn., že teoreticky by aplikace mohla být ke stažení na webu **pk-elsys.cz**. V telefonu je třeba tuhle možnost jen povolit. Tudíž, než se podaří dokončit registraci aplikace na „**Google Play**“, je možné pro zájemce aplikaci poskytnout tímto způsobem...

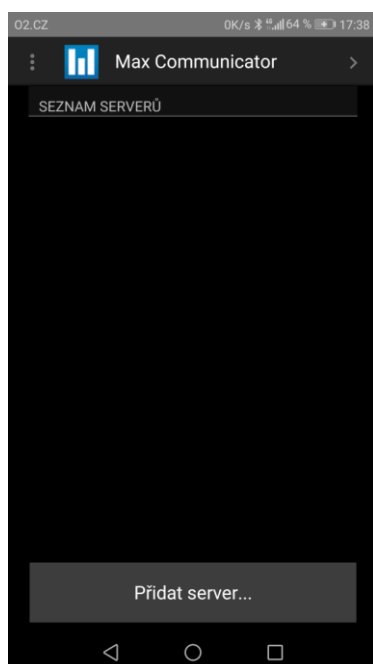
Po stažení a instalaci aplikace „**Max Communicator**“ ji spusťte. Zobrazí se úvodní startovací „okno“ (stereotypní terminologie z Windows:) aplikace s výpisem všech připojení, tzn. seznam serverů. Prvotně je seznam samozřejmě prázdný a je třeba nějaké připojení vytvořit.

Tlačítko vlevo nahoře ovládá skryté menu, které se rozbalí po klepnutí na něj – viz obrázek vpravo...

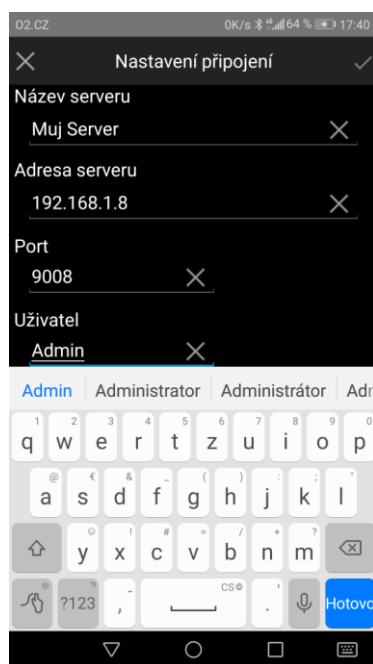
Poklepem na povel „**Nový**“ se vytvoří nový záznam a otevře se formulář pro úpravu připojení k serveru...



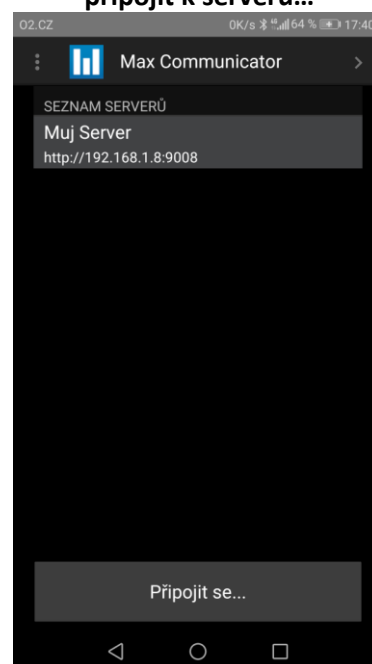
Aplikace po instalaci



Přidání nového serveru



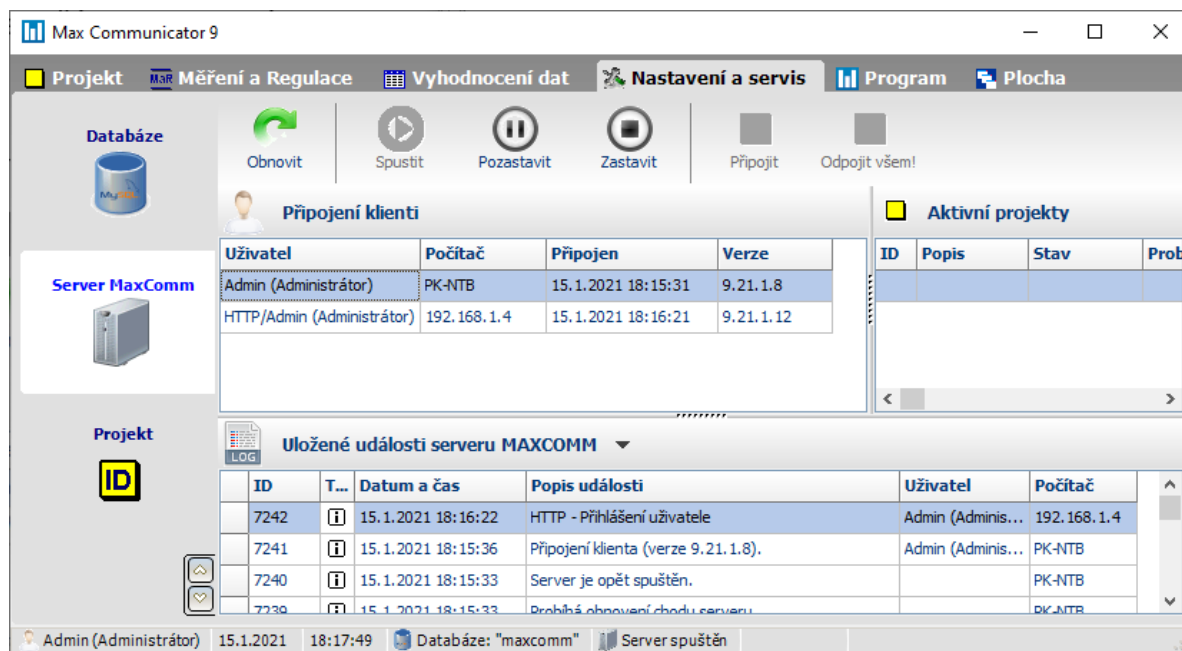
Aplikace je připravena se připojit k serveru...



Tip: Nejdříve zkuste aplikaci „rozchodit“ s telefonem připojeným přes WIFI na lokální síti. Záleží ovšem na konfiguraci sítě ve vaší firmě, zde z rozsahu adres pro síť WIFI je možné dosáhnout na počítač, kde leží HTTP server – viz příslušná kapitola o instalaci a konfiguraci MaxComm serveru...

Je-li vše v pořádku, pak po klepnutí na tlačítko „**Připojit se...**“, se aplikace připojí na HTTP server a stáhne seznam všech projektů, ke kterým má zadaný uživatel oprávnění. Aplikace se přepne na výpis projektů – viz popis na začátku tohoto návodu...

V desktopové aplikaci „**Max Communicator**“ lze vidět připojení mobilního klienta na HTTP server:



Pokud připojení nefunguje už na lokální síti, je třeba znovu ověřit, zda je:

- na počítači serveru opravdu spuštěna služba „**MaxComm server**“ – např. pomocí desktopové aplikace klienta a zda je povolen HTTP server na portu 9008.
- ve firewallu záznam o výjimce pro port 9008.
- možné otevřít hlavní webovou stránku HTTP serveru z jiného počítače v síti a pokud ano, zkuste to otevřít v prohlížeči toho telefonu připojeného přes WIFI...
- adresní rozsah WIFI totožný s rozsahem lokální sítě, případně existuje routování do tohoto rozsahu? **Pokud ne, nemá dál smysl lokální připojení přes telefon na WIFI řešit a přejít rovnou k připojení přes internet...**

Pokud experimentujete s připojením přes „**Předávaný port**“ a přes „**VPN**“, připomínám, že v prvním případě je třeba zadat **veřejnou IP adresu** vašeho internetového připojení a v tom druhém případě (**VPN**) zadejte do adresního řádku přímo **lokální adresu serveru**. Není špatné si v aplikaci vytvořit **dvě připojení s těmito rozdílnými adresami**. Ve finále se můžete rozhodnout, jaký způsob budete pak trvale používat...

Zkušenost:

Varianta s „**VPN**“ nese v průběhu času jednu záludnost – než se začnete stresovat, proč spojení zas nefunguje (?!), zkuste nejdříve spustit a připojit „**VPN klienta**“;)...

Závěrem:

Díky „*chytrému*“ routeru ASUS mně spojení přes obě varianty fungovalo hned „*na první zapnutí*“, ale dovedu si představit, že se v tom laik může trochu zamotat. Pokud je to váš případ, svěřte to odborné firmě...

Přeji, ať vám aplikace funguje, jak má! No a v opačném případě mne neváhejte kontaktovat!
Mnoho zdaru!

5 Výrobce aplikace



Ing. Petr Kobert, www.pk-elsys.cz
Kontakt: info@pk-elsys.cz
Provozovna: Olomouc