Príručka sieťových spojení pre JC-E SECURE prevodníky

(verzia dokumentu 1.31)

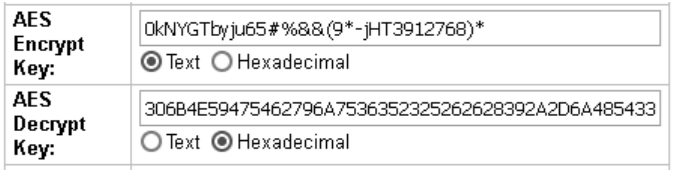
Obsah

1. Spôsoby zabezpečenia M-Bus komunikácie - tunelu (M-Bus port a Ethernet)

1.1. AES

AES (Advanced Encryption Standard) symetrický blokový šifrovací algoritmus.
Dĺžka kľúča môže byť 128, 192 alebo 256 bitov. Je určený na šifrovanie blokov dát. AES zabezpečuje dôvernosť (šifrovanie), nie integritu alebo autenticitu dát. Je možné použiť jeden kľúč pre šifrovanie (odchádzajúce dáta) a druhý kľúč pre dešifrovanie (prichádzajúce dáta) čo zvyšuje bezpečnosť šifrovania. V režime server je podporovaný TCP protokol. V režime klient sú podporované protokoly TCP a UDP. Kľúč je možné zadať ako text ASCII znakov, alebo v hexa formáte.

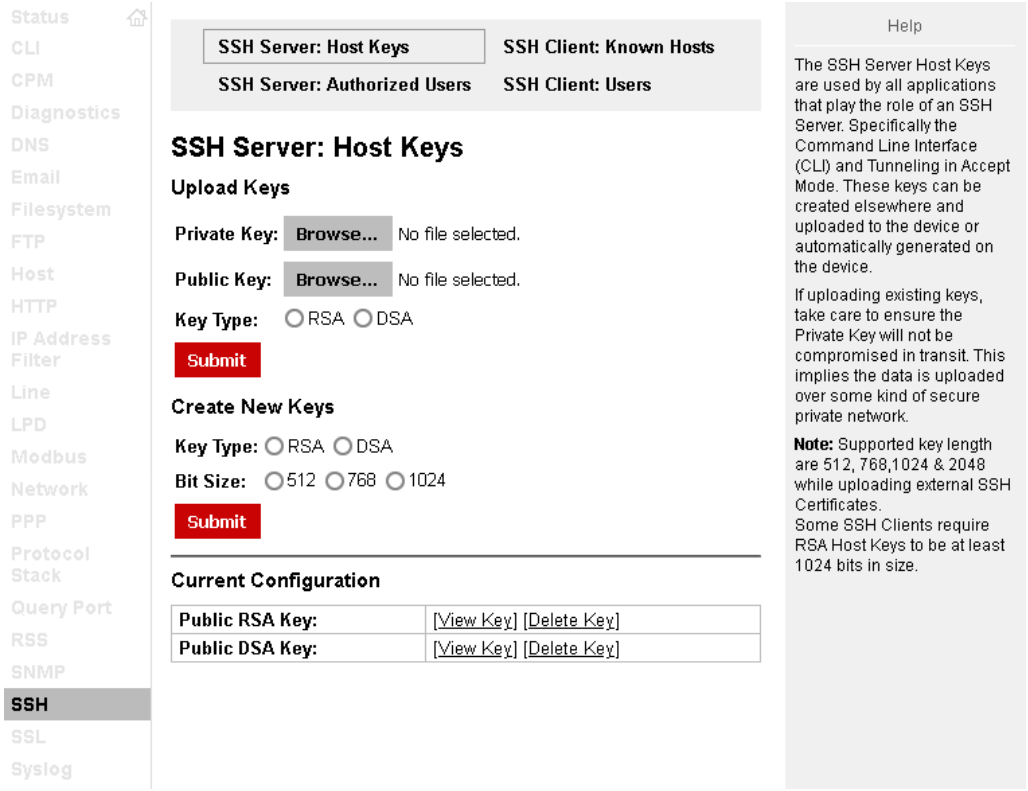
Nastavenia pre tento typ zabezpečeného spojenia sa nachádzajú vo webovom rozhraní prevodníku
ak sa má prevodní správať ako server pod Tunnel > Accept Mode > Protocol, alebo
ak sa má prevodník správať ako client pod Tunnel > Host 1 > Connect Mode > Protocol.

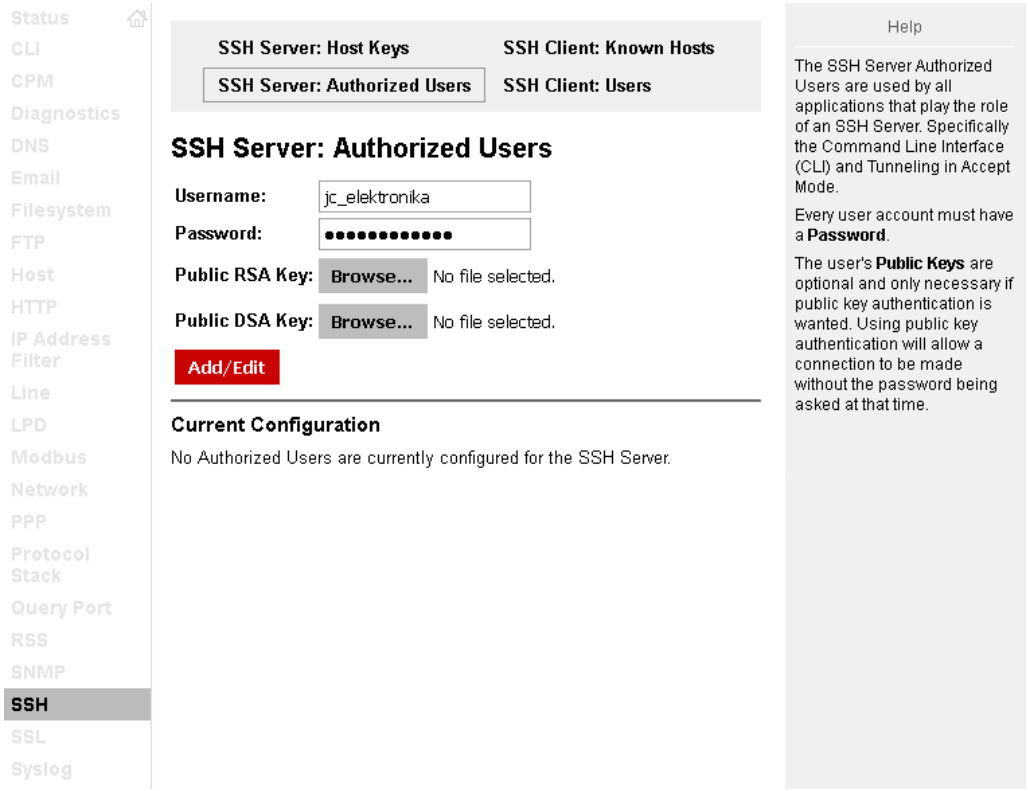


1.2. SSH

SSH je jedna z najspoľahlivejších a najbežnejších metód, ako zabezpečiť TCP spojenie. Primárne je určená pre zabezpečenie HTTPS protokolu, ale je možné aj tunelovanie M-Bus dát TCP spojením. Zabezpečuje dôvernosť (šifrovanie), integritu a autenticitu dát.

Režim server - musia byť nahrané uživateľský kľúč/kľúče a musí byť nadefinovaný minimálne jeden SSH autorizovaný užívateľ. Kľúče je možné vygenerovať v prevodníku, alebo nahrať cez webové rozhranie.
Sú podporované kľúče RSA a DSA s dĺžkou 512, 768, 1024 bitov. Užívateľ musí mať zadefinované meno a heslo.
Verejné kľúče používateľa sú voliteľné a potrebné len v prípade, ak je požadované overenie verejným kľúčom.
Použitie overenia verejným kľúčom umožní vytvorenie pripojenia bez zadania hesla v danom režime.

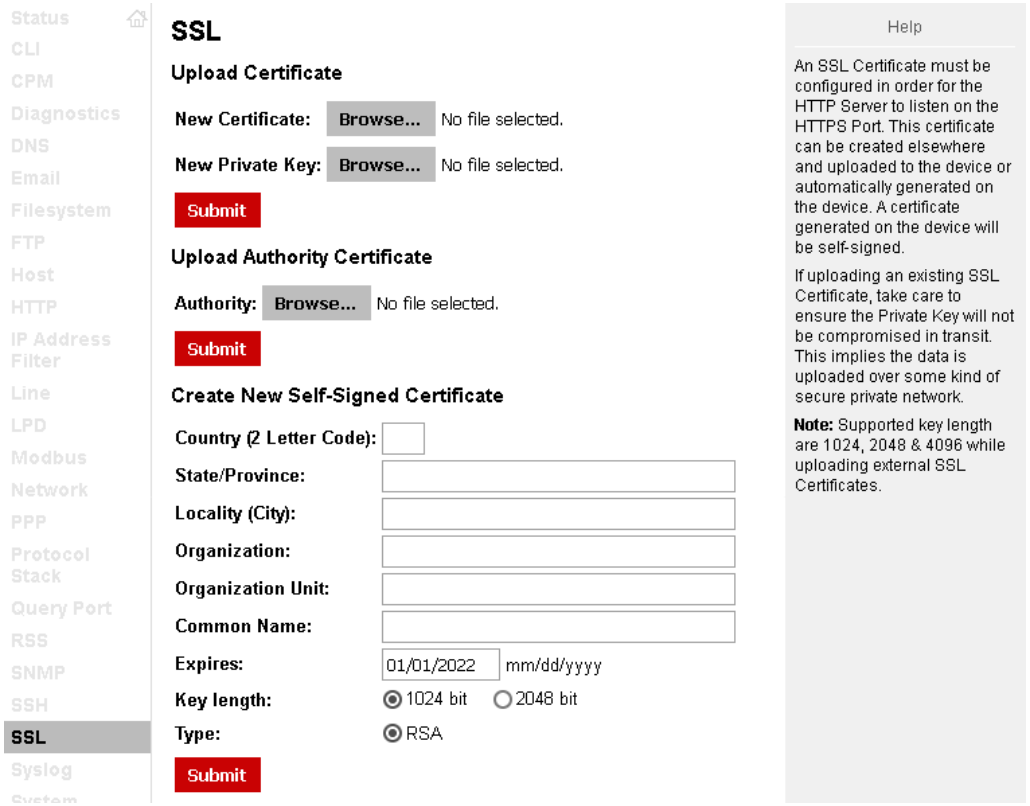




Režim client - Konfigurácia týchto verejných kľúčov je voliteľná, ale ak existujú, poskytujú ďalšiu vrstvu zabezpečenia, ktorá pomáha zabrániť útokom typu Man-in-the-Middle (MITM).
Pri pridávaní verejných kľúčov hostiteľa pre server zadajte buď DNS názov servera alebo jeho IP adresu. Názov servera by sa mal zhodovať s nastavením tunelovania.
Pre užívateľa musí byť nakonfigurované aspoň heslo alebo pár kľúčov. Kľúče pre overovanie je možné vygenerovať v prevodníku, alebo nahrať cez webové rozhranie.

1.3. SSL

SSL je univerzálny šifrovací protokol na zabezpečenie TCP/IP komunikácie. Prevodník ho môže využíť na šifrovanie HTTPS (webovej stránky), alebo tunelovanie M-Bus dát.
Zabezpečuje dôvernosť (šifrovanie), integritu a autenticitu prenášaných dát.
Prevodník podporuje TCP/IP tunelovanie v režime server aj klient.
V prevodníku je možné vygenerovať a použiť self-signed certifikát, alebo je možné nahrať vlastný certifikát spolu s autorizačným certifikátom. Self-signed certifikát je typu RSA s dĺžkou kľúča 1024, alebo 2048 bitov.



2. Zabezpečené spojenia

Existuje viacero spôsobov, ako vytvoriť zabezpečené spojenie pomocou prevodníka. Táto príručka sa zaoberá len nasledujúcimi tromi metódami:

1. TCP AES spojenie s prevodníkom ako serverom a aplikáciou virtuálneho sériového COM portu ako klientom.
2. SSL pripojenie s prevodníkom ako klientom.
3. SSL pripojenie s prevodníkom ako serverom.

Na vytvorenie SSL spojenia bude použitá aplikácia s názvom stunnel pre Windows.

Inštalačný program pre stunnel je možné stiahnuť tu:
https://www.stunnel.org/downloads.html

Základné informácie o programe stunnel:
https://www.stunnel.org/howto.html

Podrobné informácie o nastaveniach programu stunnel:
https://www.stunnel.org/static/stunnel.html

Nie je to potrebné, ale na testovanie a riešenie problémov so spojením je možné použiť open source nástroj s názvom TCP/IP builder. Viac informácií nájdete tu:
https://www.drk.com.ar/en/legacy/tcp-ip-builder/

2.1. TCP AES s prevodníkom ako serverom a virtuálnym COM portom ako klientom

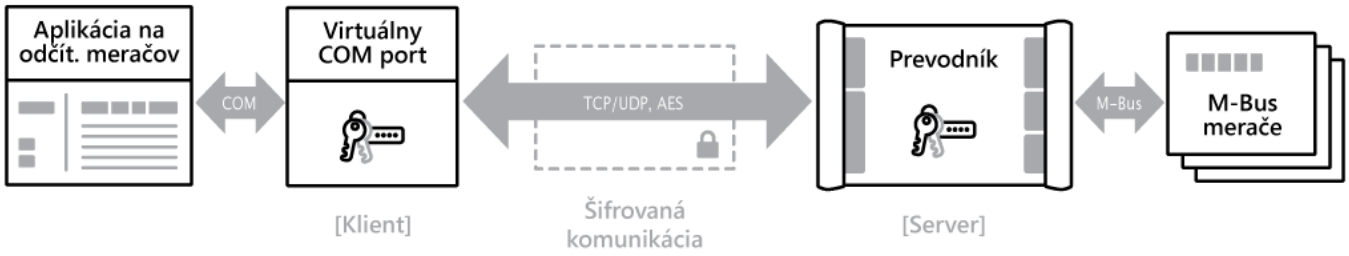


Diagram TCP AES spojenia s prevodníkom ako serverom a virtuálnym COM portom ako klientom

Na oboch stranách je použitý rovnaký šifrovací kľúč.

⚠ Dôležitá poznámka:
Firewall používaný v systéme Windows alebo kdekoľvek inde v reťazci spojenia musí byť správne nakonfigurovaný, aby pripojenie nebolo blokované. Ak sa pripojenie nedá nadviazať napriek správnym nastaveniam, je potrebné dôkladne skontrolovať konfiguráciu firewall-u.

2.1.1 Prevodník ako server s TCP AES

Postup konfigurácie:

1. Otvorte webové rozhranie prevodníka v webovom prehliadači
   Štandardná IP adresa je 169.254.100.10
2. Otvorte nastavenia T**unel** v ľavom bočnom paneli.
3. Otvorte nastavenie **Accept Mode**
4. Nastavte nasledujúce nastavenia:

   Mode: Always

   Local port: 10001 (alebo akékoľvek iné požadované číslo portu)

   Protocol: TCP AES

   AES Encrypt Key: Zadajte kľúč v hexadecimálnom formáte, dĺžka 128 bitov, 32 hex znakov bez medzier.
   napr. 00112233445566778899aabbccddeeff

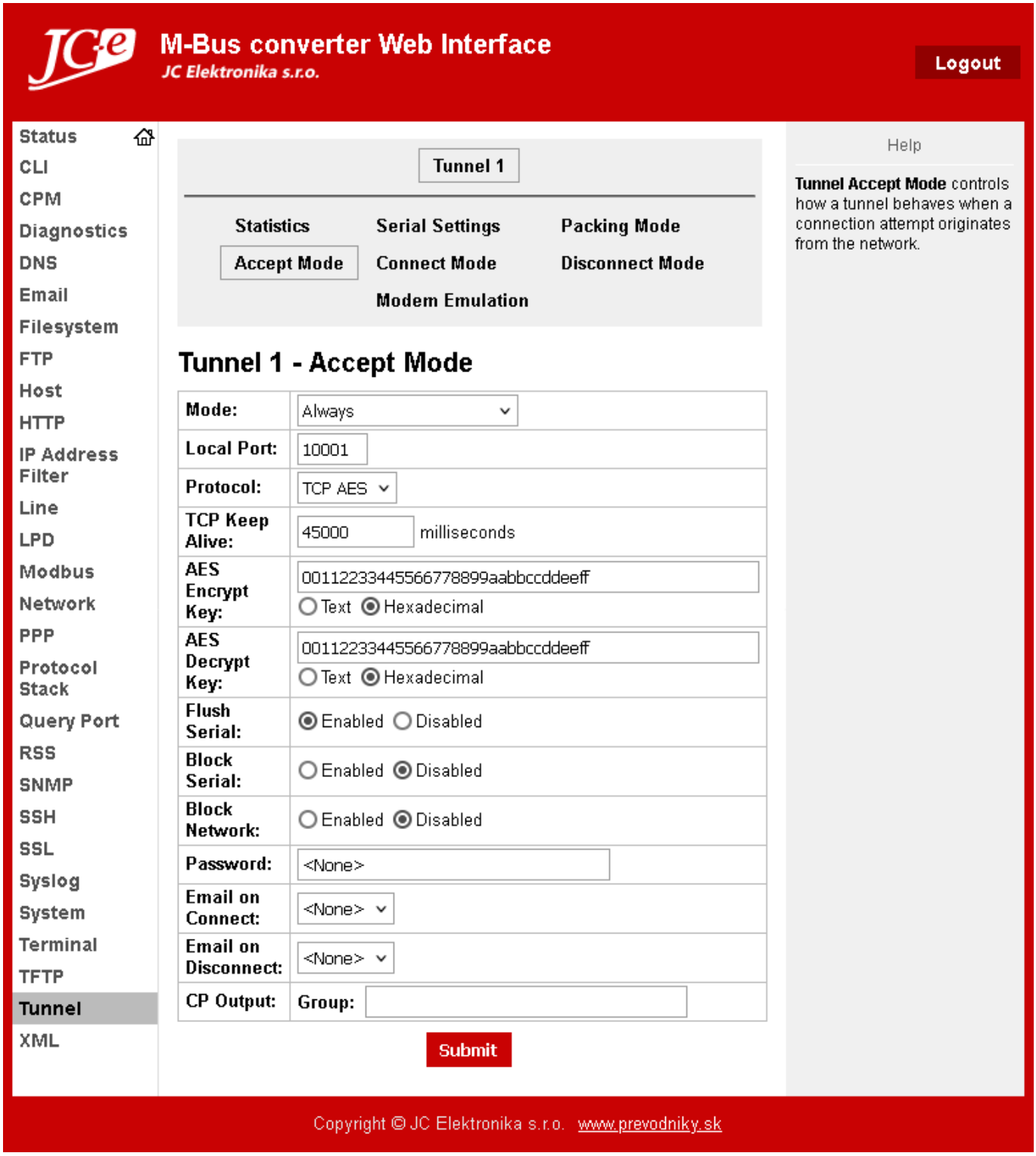
   Format: ◉ Hexadecimal

   AES Decrypt Key: Zadajte rovnaký kľúč ako v Encrypt Key

   Format: ◉ Hexadecimal

   Ostatné nastavenia nie je potrebné meniť, pokiaľ to nie je žiadúce.

5. Kliknite na **Submit**.



2.1.2 Lantronix Secure Com Port Redirector klient

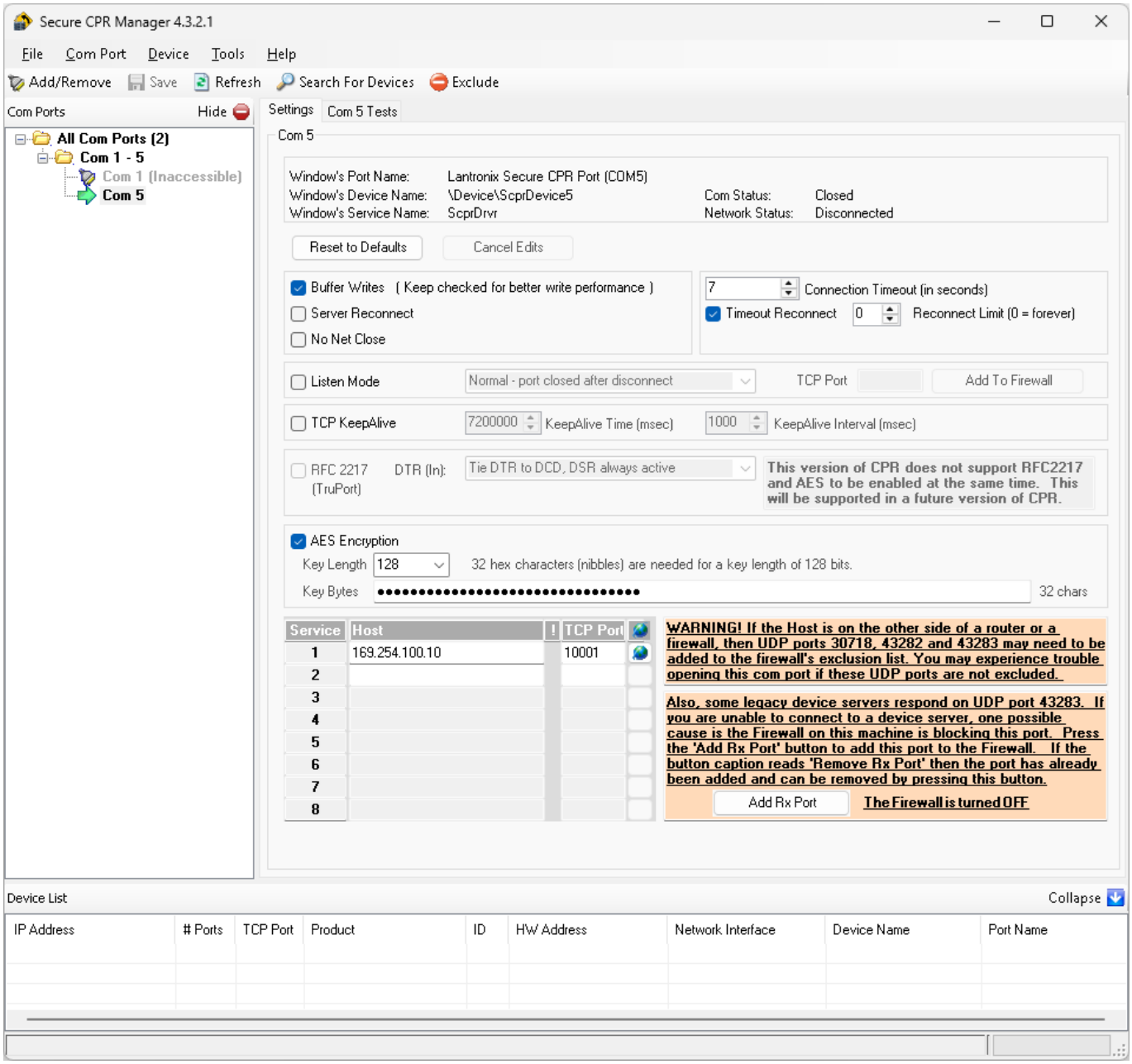
Na vytvorenie virtuálneho sériového portu použijeme aplikáciu Lantronix Secure Com Port Redirector.
Túto aplikáciu si môžete stiahnuť napríklad tu:
https://papouch.com/lantronix-secure-com-port-redirector-p7194/

Postup konfigurácie:

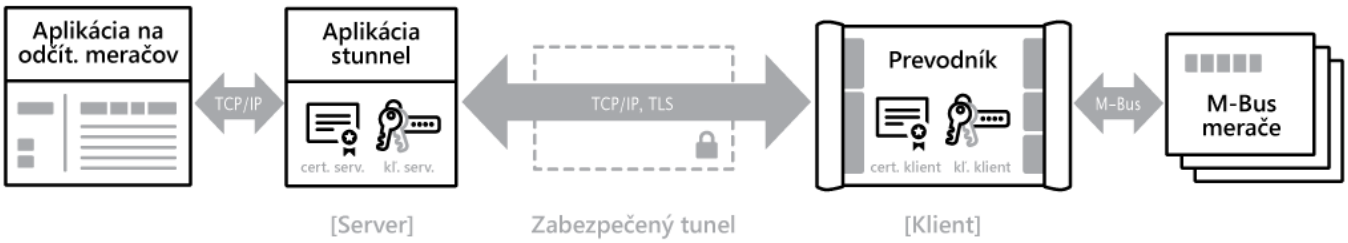
1. Spustite applikáciu Lantronix Secure Com Port Redirector.
2. Kliknite na tlačidlo **Add/Remove** na paneli nástrojov, týmto pridáte COM port.

3. Vyberte vytvorený port, napr. **COM 5**, v ľavom bočnom paneli.
4. Zaškrtnite políčko **AES Encrytion.**
5. Nastavte **Key length:** 128 bitov.
6. Nastavte **Key bytes:** Zadajte kľúč v hexadecimálnom formáte, 32 hex znakov bez medzier.
   napr. 00112233445566778899aabbccddeeff

   Kľúč musí byť zhodný so šifrovacím a aj dešifrovacím kľúčom používaným v prevodníku.
7. V tabuľke Service nastavte jeden riadok
   Host: 169.254.100.10 (IP adresa prevodníka)
   TCP Port: 10001 (port prevodníka)
8. V hornom paneli nástrojov kliknite na tlačidlo **Save**.



2.2. SSL s prevodníkom ako klientom a stunnel-om ako serverom



SSL spojenie s prevodníkom ako klientom a stunnel-om ako server.

Prevodník by mal používať svoj vlastný certifikát a privátny kľúč. Aplikácia stunnel alebo akákoľvek iná aplikácia, ktorá ju nahrádza (napríklad systém SCADA), by mala používať vlastný certifikát a privátny kľúč, ktoré sa odlišujú od tých ktoré sú použité na prevodníku.

Poznámka: Použitie zabezpečeného spojenia zvyšuje oneskorenie prenosu dát o 5 ms.

⚠ Dôležitá poznámka:
Firewall používaný v systéme Windows alebo kdekoľvek inde v reťazci spojenia musí byť správne nakonfigurovaný, aby pripojenie nebolo blokované. Ak sa pripojenie nedá nadviazať napriek správnym nastaveniam, je potrebné dôkladne skontrolovať konfiguráciu firewall-u.

2.2.1 Prevodník ako klient s SSL

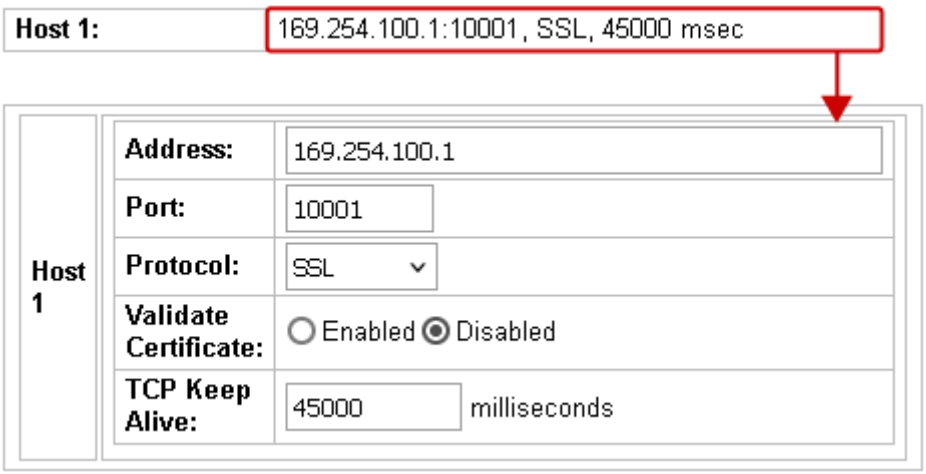
Postup konfigurácie prevodníka ako klienta:

1. Otvorte webové rozhranie prevodníka v webovom prehliadači.
   Štandardná IP adresa je 169.254.100.10
2. Nastavte certifikát SSL a privátny kľúč v konfigurácii SSL.
   Viď kapitola: Konfigurácia SSL.
3. Otvorte nastavenie **Tunel** v ľavom bočnom paneli.
4. Otvorte nastavenie **Connect Mode**.
5. Nastavte nasledujúce:

   Mode: Always

   Local Port: Nechajte prázdne.

   Host 1: Kliknutím na bunku tabuľky otvoríte podrobné nastavenia pre Host 1.



Pre Host 1 nastavte:

Address: 169.254.100.1 (IP adresa stunnel servera)

Port: 10001 (port stunnel servera)

Protocol: SSL

Validate Certificate: Disabled

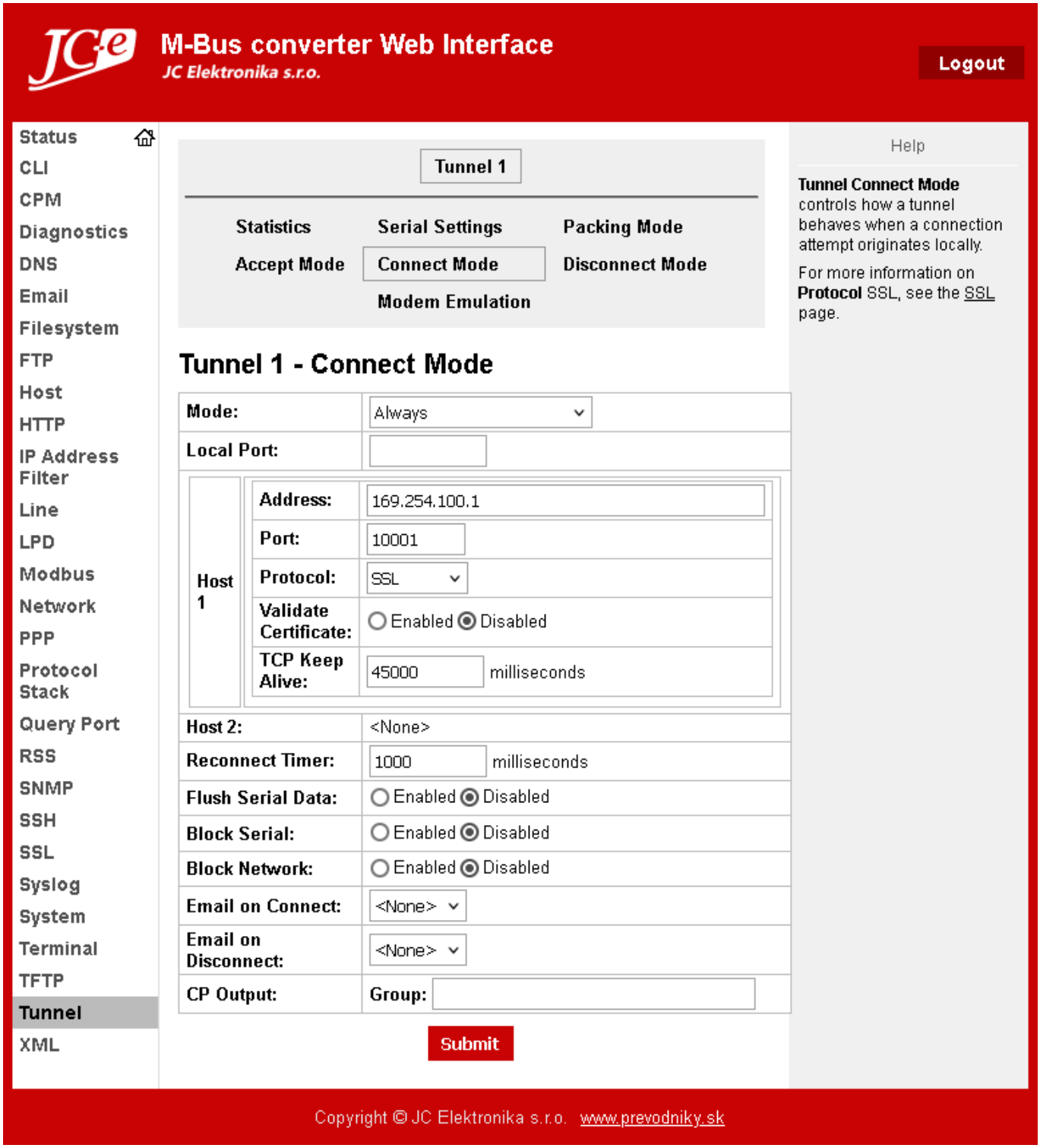
Poznámka:
Ak chcete povoliť overovanie certifikátov, musíte prejsť do nastavení **SSL** a v sekcii **Upload Authority Certificate** pridať certifikát používaný programom stunnel do certifikačnej autority.

Certifikát stunnel servera (`cert_stunnel.pem`) je v danom nastavení potrebné pridať, aby ho prevodník mohol použiť na overenie. Do prevodníka je možné pridať viacero certifikátov do jeho interného úložiska certifikátov. To sa vykoná výberom jedného samostatného súboru certifikátu a kliknutím tlačidla Submit. Tento postup sa opakuje pre viacero súborov.

Ostatné nastavenia nie je potrebné meniť, pokiaľ to nie je žiadúce.

6. Kliknite na **Submit**.

   Prevodník sa bude pravidelne pokúšať vytvoriť spojenie so serverom v časovom intervale podľa nastavenia Reconnect Timer, ktorý je štandardne nastavený na 1 sekundu.



2.2.2 Stunnel server s SSL

Na vytvorenie servera použijeme aplikáciu stunnel. Viac informácií nájdete v úvode kapitoly Zabezpečené spojenia.

Postup konfigurácie stunnel servera:

1. Vytvorte privátny šifrovací kľúč a certifikát pre použitie v stunnel-i.
   Viď kapitola: Vytvorenie privátneho kľúča a samo-podpísaného certifikátu.
   Ak ste ich už vytvorili počas konfigurácie prevodníka, môžete pokračovať bodom 2.

2. Otvorte stunnel cez Windows ponuku Štart, odkaz **stunnel GUI start**.

3. Upravte konfiguráciu stunnel-u. V hlavnom menu vyberte **Configuration > Edit configuration**.

   Aplikácia obsahuje vzorovú konfiguráciu v súbore stunnel.conf. Všetky sekcie zakomentujte pomocou bodkočiarky (;) na začiatku každého riadka alebo zazálohujte celý súbor a vytvorte úplne nový súbor `stunnel.conf`, ktorý bude obsahovať len vašu vlastnú konfiguráciu.

4. Pridajte nasledujúce riadky do konfiguračného súboru, zmeňte hodnoty IP adries a portov podľa svojich potrieb.

```
[stunnelserver]
accept = 169.254.100.1:10001
connect = 127.0.0.1:10002
cert = cert_stunnel.pem
key = key_stunnel.pem
```

5. Ak potrebujete validáciu certifikátu pomocou certifikačnej autority, pridajte nasledujúce riadky.

```
verify = 0
verifyChain = yes
verifyPeer = yes
CAfile = ca_cert_converter.pem
```

   Súbor `ca_cert_converter.pem` je ten istý súbor certifikátu, aký používa prevodník.

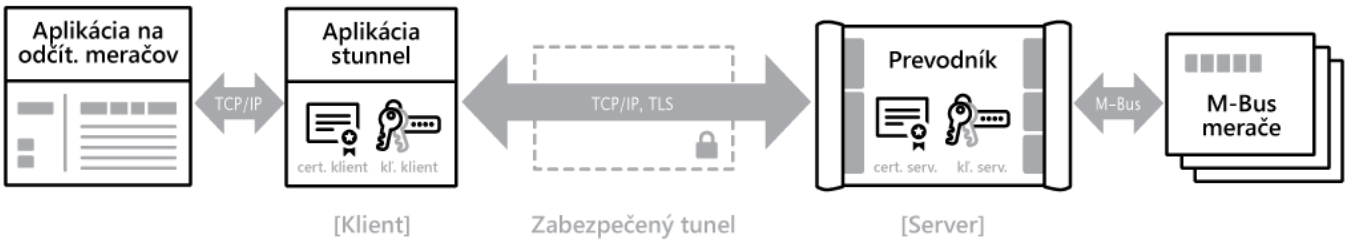
   V jednom súbore môže byť uložených viacero certifikátov alebo na overenie môže byť použitý adresár obsahujúci viacero certifikátov, popis takéhoto nastavenia nie je súčasťou tejto príručky.

   Viac informácií o možnostiach nastavenia stunnel-u nájdete tu:
   https://www.stunnel.org/static/stunnel.html

6. V hlavnom menu stunnel-u zvoľte **Configuration** > **Reload configuration**.

   Po tomto kroku by mal byť Stunnel pripravený prijať pripojenie z prevodníka.

2.3. SSL s prevodníkom ako serverom a stunnel-om ako klientom



SSL spojenie s prevodníkom ako serverom a stunnel-om ako klientom.

Prevodník by mal používať svoj vlastný certifikát a privátny kľúč. Aplikácia stunnel alebo akákoľvek iná aplikácia, ktorá ju nahrádza (napríklad systém SCADA), by mala používať vlastný certifikát a privátny kľúč, ktoré sa odlišujú od tých ktoré sú použité na prevodníku.

Poznámka: Použitie zabezpečeného spojenia zvyšuje oneskorenie prenosu dát o 5 ms.

⚠ **Dôležitá poznámka:**
Firewall používaný v systéme Windows alebo kdekoľvek inde v reťazci spojenia musí byť správne nakonfigurovaný, aby pripojenie nebolo blokované. Ak sa pripojenie nedá nadviazať napriek správnym nastaveniam, je potrebné dôkladne skontrolovať konfiguráciu firewall-u.

2.3.1 Prevodník ako server s SSL

Keď bude prevodník fungovať ako server s SSL, bude potrebné, aby bol na prevodníku prítomný privátny šifrovací kľúč a certifikát. Je možné použiť samo-podpísaný certifikát, ktorý sa dá vygenerovať interne na prevodníku, alebo je možné použiť vlastný certifikát.

Pri uploadovaní vlastného certifikátu a privátneho kľúča dbajte na to, aby nedošlo k úniku privátneho kľúča počas prenosu. To znamená, použitie bezpečnej súkromnej siete na prenos týchto súborov.

Postup konfigurácie prevodníka servera:

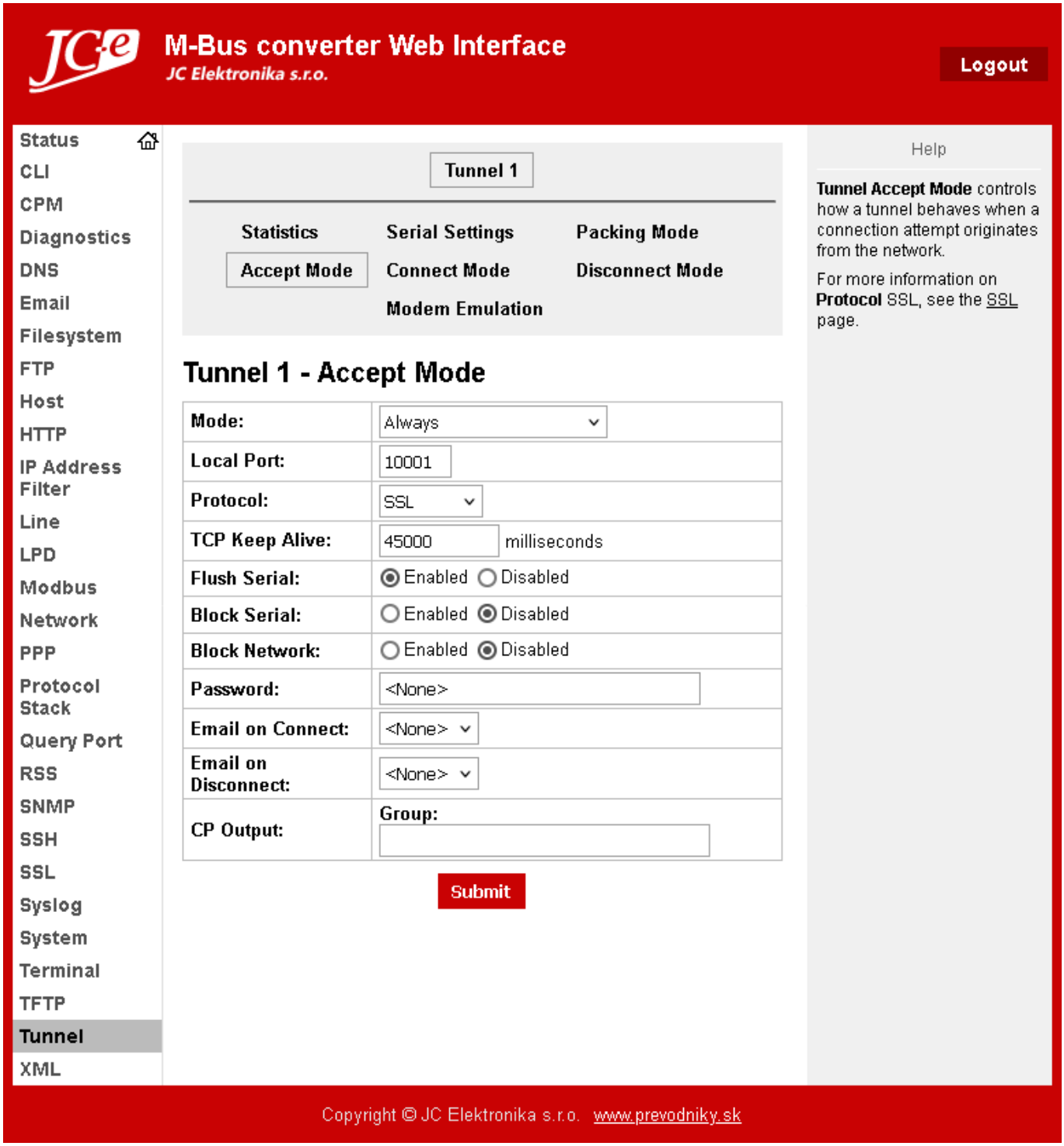
1. Otvorte webové rozhranie prevodníka v webovom prehliadači.
   Štandardná IP adresa je 169.254.100.10
2. Nastavte certifikát SSL a privátny kľúč v konfigurácii SSL.
   Viď kapitola: Konfigurácia SSL.
3. Otvorte nastavenie **Tunel** v ľavom bočnom paneli.
4. Otvorte nastavenie **Accept Mode**.
5. Nastavte nasledujúce:

   Mode: Always

   Local Port: 10001 (Port ku ktorému sa pripojí stunnel klient)

   Protocol: SSL

   Ostatné nastavenia nie je potrebné meniť, pokiaľ to nie je žiadúce.
6. Kliknite na **Submit**.



2.3.2 Stunnel klient s SSL

Na vytvorenie servera použijeme aplikáciu stunnel. Viac informácií nájdete v úvode kapitoly Zabezpečené spojenia.

Postup konfigurácie stunnel klienta:

1. Vytvorte privátny šifrovací kľúč a certifikát pre použitie v stunnel-i.
   Viď kapitola: Vytvorenie privátneho kľúča a samo-podpísaného certifikátu.
   Ak ste ich už vytvorili počas konfigurácie prevodníka, môžete pokračovať bodom 2.

2. Otvorte stunnel cez Windows ponuku Štart, odkaz **stunnel GUI start**.

3. Upravte konfiguráciu stunnel-u. V hlavnom menu vyberte **Configuration > Edit configuration**.

   Aplikácia obsahuje vzorovú konfiguráciu v súbore stunnel.conf. Všetky sekcie zakomentujte pomocou bodkočiarky (;) na začiatku každého riadka alebo zazálohujte celý súbor a vytvorte úplne nový súbor `stunnel.conf`, ktorý bude obsahovať len vašu vlastnú konfiguráciu.

4. Pridajte nasledujúce riadky do konfiguračného súboru, zmeňte hodnoty IP adries a portov podľa svojich potrieb.

```
[stunnelclient]
accept = 127.0.0.1:10001
connect = 169.254.100.10:10001
client = yes
verify = 0
cert = cert_stunnel.pem
key = key_stunnel.pem
sslVersion = TLSv1.2
options = LEGACY_SERVER_CONNECT
options = NO_TICKET
options = DONT_INSERT_EMPTY_FRAGMENTS
```

5. Ak potrebujete validáciu certifikátu pomocou certifikačnej autority, pridajte nasledujúce riadky.

```
verifyChain = yes
verifyPeer = yes
CAfile = ca_cert_converter.pem
```

   Súbor `ca_cert_converter.pem` je ten istý súbor certifikátu, aký používa prevodník.

   V jednom súbore môže byť uložených viacero certifikátov alebo na overenie môže byť použitý adresár obsahujúci viacero certifikátov, popis takéhoto nastavenia nie je súčasťou tejto príručky.

   Viac informácií o možnostiach nastavenia stunnel-u nájdete tu:
   https://www.stunnel.org/static/stunnel.html

6. V hlavnom menu stunnel-u zvoľte **Configuration** > **Reload configuration**.

   Po tomto kroku by mal stunnel byť pripravený na vytvorenie spojenia s prevodníkom fungujúcim ako server. Spojenie s prevodníkom bude vytvorené až po nadviazaní spojenia medzi stunnel aplikáciou a aplikáciou na odčítanie meračov.

3. HTTPS pre webové rozhranie prevodníka

Na povolenie prístupu cez HTTPS je potrebné nakonfigurovať SSL certifikát a privátny šifrovací kľúč. Je možné použiť samo-podpísaný certifikát, ktorý sa dá vygenerovať interne na prevodníku, alebo je možné použiť vlastný certifikát.

Viď kapitola: Konfigurácia SSL.

Po nastavení SSL sa stane prístup cez HTTPS dostupný.

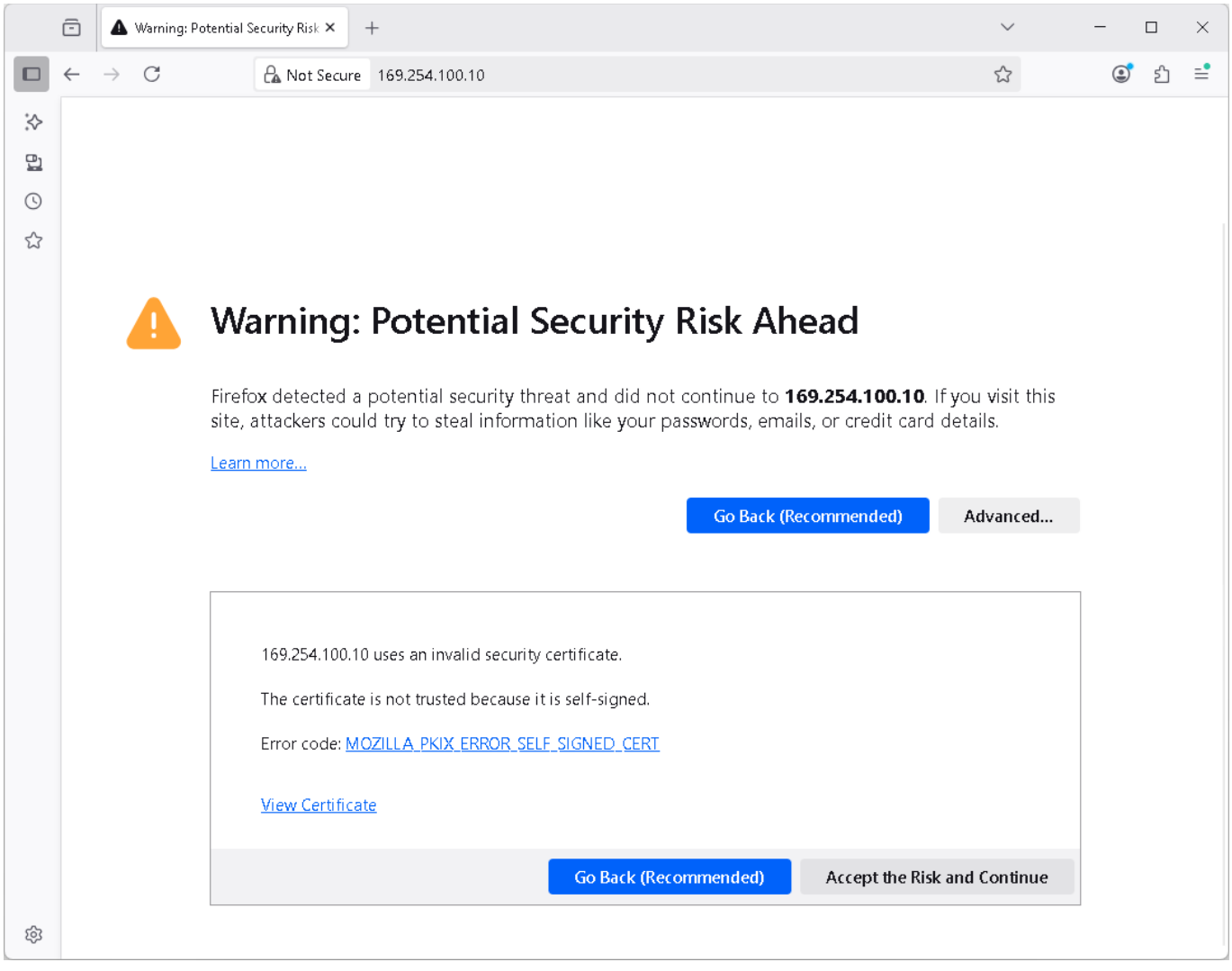
Pri uploadovaní vlastného certifikátu a privátneho kľúča dbajte na to, aby nedošlo k úniku privátneho kľúča počas prenosu. To znamená, použitie bezpečnej súkromnej siete na prenos týchto súborov.

Podporované dĺžky kľúčov sú 1024, 2048 a 4096 bitov s externými certifikátmi SSL.

⚠ Dôležitá poznámka:
Pri použití kľúčov väčších ako 1024 bitov dochádza k spomaleniu odozvy cez HTTPS a načítanie webového rozhrania prevodníka môže trvať nadmerne dlho.

Pri použití samo-podpísaného certifikátu budete musieť pri otvorení webového rozhrania cez HTTPS prijať jednorazové bezpečnostné upozornenie vo vašom webovom prehliadači.

V webovom prehliadači kliknite na **Pokročilé...** > **Akceptovať riziko a pokračovať**.



3.1. Vypnutie nezabezpečeného protokolu HTTP.

Postup vypnutia nezabezpečeného prístupu cez protokol HTTP:

1. Otvorte webové rozhranie prevodníka v webovom prehliadači.
   Štandardná IP adresa je 169.254.100.10
2. Otvorte nastavenie **HTTP** v ľavom bočnom paneli.
3. Zvoľte **Configuration**.
4. Nastavte **Port** na 0.
5. Kliknite na **Submit**.

Poznámka:
Po vykonaní tejto operácie sa stane webové rozhranie prostredníctvom nezabezpečeného HTTP pripojenia nedostupné. Budete musieť do adresného riadka zadať adresu s https:// a webové rozhranie otvoriť znovu.


M-Bus converter Web Interface
JC Elektronika s.r.o.
Logout
Status
CLI
CPM
Diagnostics
DNS
Email
Filesystem
FTP
Host
HTTP
IP Address Filter
Line
LPD
Modbus
Network
PPP
Protocol Stack
Query Port
RSS
SNMP
SSH
SSL
Syslog
System
Terminal
TFTP
Tunnel
XML
Statistics
Configuration
Authentication
HTTP Configuration
State: Enabled Disabled
Port: 0
Secure Port: 443
Secure Protocols: TLS1.0 TLS1.1 TLS1.2
Max Timeout: 10 seconds
Max Bytes: 40960
Logging State: Enabled Disabled
Max Log Entries: 50
Log Format: %h %t "%r" %s %B "%{Referer}i" "%{User-Agent
Authentication Timeout: 30 minutes
Help
This page displays and changes the current HTTP Configuration settings.
Copyright © JC Elektronika s.r.o. www.prevodniky.sk

4. Konfigurácia SSL

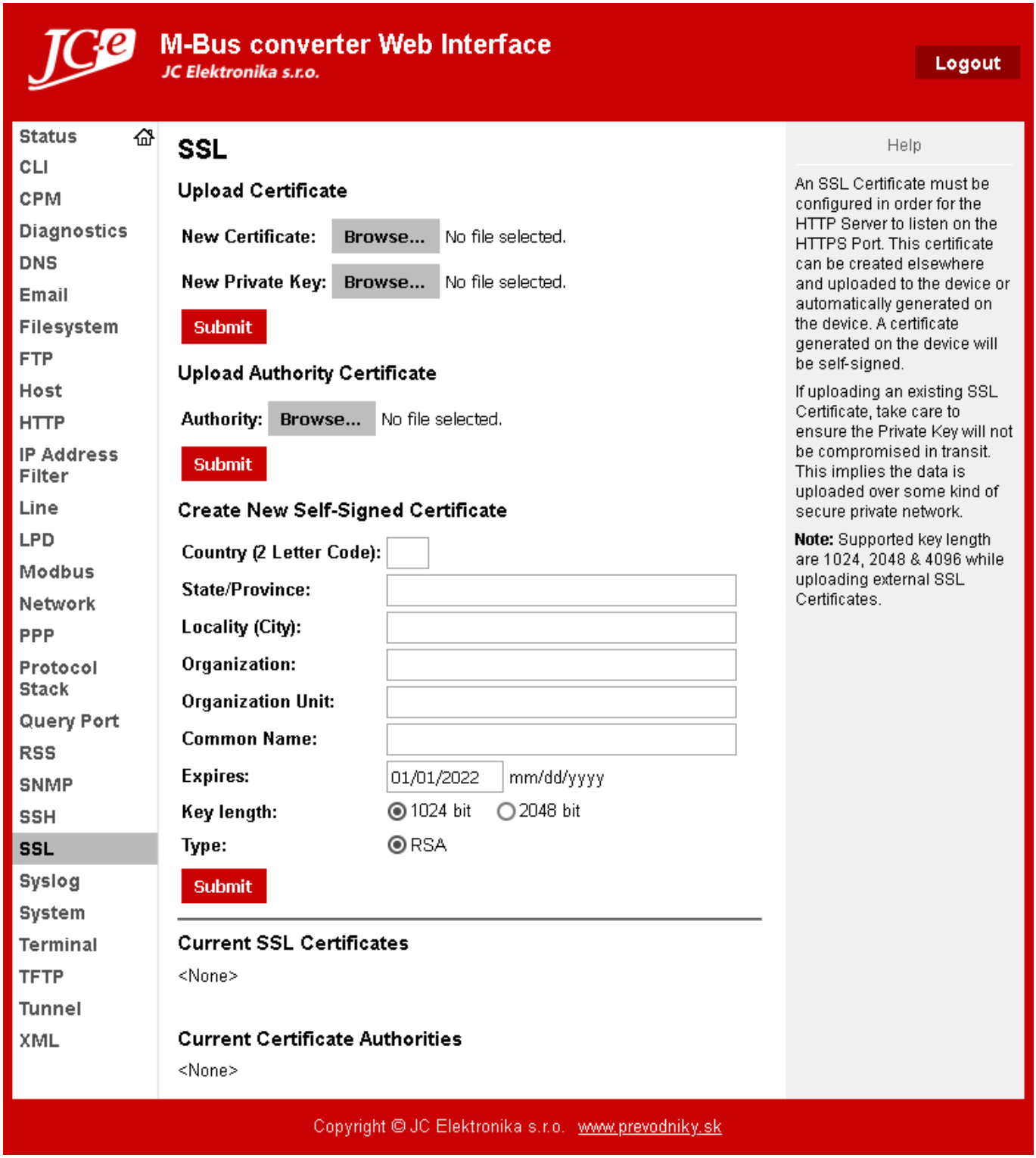
Aby bolo možné používať SSL tunelovanie na prenos dát alebo HTTPS na prístup k webovému rozhraniu, je potrebné nakonfigurovať SSL certifikát a privátny šifrovací kľúč. Prevodník môže interne vygenerovať vlastný certifikát a kľúč alebo je možné do prevodníka nahrať externý certifikát a kľúč.

Postup vytvorenia interne generovaného certifikátu:

1. Otvorte webové rozhranie prevodníka v webovom prehliadači.
   Štandardná IP adresa je 169.254.100.10
2. Otvorte nastavenia **SSL** v ľavom bočnom paneli.
3. V sekcii **Create New Self-Signed Certificate** vyplňte všetky požadované údaje:
   Country (2 Letter Code) - Krajina (2-písmenový kód)
   State/Province - Štát/provincia (kraj)
   Organization - Organizácia
   Organization Unit - Organizačná jednotka (oddelenie)
   Common Name - Bežný názov
   Expires - Platnosť
   Key length - Dĺžka kľúča
4. Kliknite na tlačidlo **Submit** v sekcii **Create New Self-Signed Certificate**.

Postup pre nahranie vlastného certifikátu:

1. Vytvorte privátny šifrovací kľúč a certifikát,
   Viď kapitola: Vytvorenie privátneho kľúča a samo-podpísaného certifikátu.
2. Otvorte webové rozhranie prevodníka v webovom prehliadači.
   Štandardná IP adresa je 169.254.100.10
3. Otvorte nastavenia **SSL** v ľavom bočnom paneli.
4. V nastavení **New Certificate** kliknite na tlačidlo **Browse...** a zvoľte súbor certifikátu (`cert_converter.pem`).
5. V nastavení **New Private Key** kliknite na tlačidlo **Browse...** a zvoľte súbor kľúča (`key_pkcs8_converter.pem`).
6. Kliknite na tlačidlo **Submit** v sekcii **Upload Certificate**.


M-Bus converter Web Interface
JC Elektronika s.r.o.
Logout
Status
CLI
CPM
Diagnostics
DNS
Email
Filesystem
FTP
Host
HTTP
IP Address Filter
Line
LPD
Modbus
Network
PPP
Protocol Stack
Query Port
RSS
SNMP
SSH
SSL
Syslog
System
Terminal
TFTP
Tunnel
XML
SSL
Upload Certificate
New Certificate: Browse... No file selected.
New Private Key: Browse... No file selected.
Submit
Upload Authority Certificate
Authority: Browse... No file selected.
Submit
Create New Self-Signed Certificate
Country (2 Letter Code):
State/Province:
Locality (City):
Organization:
Organization Unit:
Common Name:
Expires: 01/01/2022 mm/dd/yyyy
Key length: 1024 bit 2048 bit
Type: RSA
Submit
Current SSL Certificates
<None>
Current Certificate Authorities
<None>
Help
An SSL Certificate must be configured in order for the HTTP Server to listen on the HTTPS Port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed.
If uploading an existing SSL Certificate, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Note: Supported key length are 1024, 2048 & 4096 while uploading external SSL Certificates.
Copyright © JC Elektronika s.r.o. www.prevodniky.sk

5. Vytvorenie privátneho kľúča a samo-podpísaného certifikátu

Na vytvorenie privátneho šifrovacieho kľúča a samo-podpísaného certifikátu budeme používať nástroj openssl z príkazového riadku.

Openssl je súčasťou balíka aplikácie stunnel, ak máte nainštalovaný stunnel, jeho inštalácia by nemala byť potrebná. Ako samostatný nástroj ho môžete stiahnuť tu: https://openssl-library.org/source/

Dokumentácia k tomuto nástroju je k dispozícii tu:
https://wiki.openssl.org/index.php/Command_Line_Utilities

Prevodník vyžaduje, aby bol kľúč uložený vo formáte PKCS#8. Openssl disponuje interným konverzným nástrojom, ktorý dokáže kľúč previesť do tohto formátu. Viac informácií nájdete tu:
https://docs.openssl.org/master/man1/openssl-pkcs8/

Poznámka:
Pre aplikáciu stunnel a prevodník by sa mali vygenerovať samostatné certifikáty a kľúče.
Podľa nižšie uvedených krokov by sa mali vygenerovať jednotlivé súbory pre obe strany:
`cert_stunnel.pem`, `key_stunnel.pem` for the stunnel
`cert_converter.pem`, `key_pkcs8_converter.pem` for the converter

Postup vytvorenia privátneho kľúča a certifikátu:

1. Otvorte príkazový riadok ako správca.
   V ponuke Štart systémy Windows vyhľadajte **Príkazový riadok**, kliknite naň pravým tlačidlom myši a vyberte možnosť **Spustiť ako správca**.

   Poznámka:
   Toto je potrebné len v prípade, ak ste nainštalovali stunnel do priečinka C:\Program Files (x86)\stunnel, pretože táto lokalita vyžaduje správcovské oprávnenia na vytváranie alebo zmenu súborov.

2. Prejdite do priečinka openssl pomocou tohto príkazu:

```
cd C:\Program Files (x86)\stunnel\bin
```

3. Vytvorte kľúč a certifikát pomocou openssl zadaním nasledujúceho príkazu:

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -sha256 -days 365
```

   Poznámka:
   Prevodník podporuje dĺžky kľúčov 1024, 2048 a 4096, ktoré je možné nastaviť pomocou parametra `rsa:` .
   Aplikácia stunnel vyžaduje kľúč s dĺžkou minimálne 2048 bitov.

4. Zadajte údaje certifikátu, ak polia zostanú prázdne, použijú sa predvolené hodnoty (zobrazené v zátvorkách):

```
Country Name (2 letters code):
State or Province (full name):
Locality Name (eg, city):
Organization Name (eg, company):
Organizational Unit Name (eg, section):
Common Name (eg, server FQDN or YOUR name):
Email Address:
```

5. Aby bolo možné kľúč použiť v prevodníku, je potrebné ho skonvertovať do formátu pkcs8.
   Tento príkaz skonvertuje súbor `key.pem` a uloží ho do nového súboru s názvom `key_pkcs8.pem`.

```
openssl pkcs8 -in key.pem -nocrypt -traditional -out key_pkcs8.pem
```

Poznámka:
Formát kľúča nie je potrebné meniť, ak sa používa s stunnell-om.

6. Premenujte súbory podľa ich cieľového zariadenia.
   To je možné vykonať v Správcovi súborov Windows alebo pomocou nasledujúcich príkazov:

   Pre prevodník

```
ren cert.pem cert_converter.pem
ren key_pkcs8.pem key_pkcs8_converter.pem
```

   Pre stunnel je potrebné vygenerovať samostatný certifikát a kľúč.
   Opakujte postup od kroku 3. Potom premenujte novo vytvorené súbory.

```
ren cert.pem cert_stunnel.pem
ren key.pem key_stunnel.pem
```

7. Aby bolo možné kľúč a certifikát použiť v aplikácii stunnel, je potrebné ich presunúť.
   `z` `C:\Program Files (x86)\stunnel\bin`
   `do` `C:\Program Files (x86)\stunnel\config`

   To je možné vykonať v Správcovi súborov Windows alebo pomocou nasledujúcich príkazov:

```
move /Y cert_stunnel.pem "C:\Program Files (x86)\stunnel\config"
move /Y key_stunnel.pem "C:\Program Files (x86)\stunnel\config"
```

8. Ak budete chcieť používať overovanie certifikátov, skopírujte certifikát prevodníka do priečinka `config` s novým názvom `ca_cert_converter.pem`.

```
copy /Y cert_converter.pem "C:\Program Files (x86)\stunnel\config\ca_cert_converter.pem"
```