

Príručka siet'ových spojení pre JC-E SECURE prevodníky

(verzia dokumentu 1.31)

Obsah

1. Spôsoby zabezpečenia M-Bus komunikácie - tunelu (M-Bus port a Ethernet).....	2
1.1. AES.....	2
1.2. SSH.....	2
1.3. SSL.....	4
2. Zabezpečené spojenia.....	5
2.1. TCP AES s prevodníkom ako serverom a virtuálnym COM portom ako klientom.....	6
2.1.1 Prevodník ako server s TCP AES.....	6
2.1.2 Lantronix Secure Com Port Redirector klient.....	7
2.2. SSL s prevodníkom ako klientom a stunnel-om ako serverom.....	9
2.2.1 Prevodník ako klient s SSL.....	9
2.2.2 Stunnel server s SSL.....	11
2.3. SSL s prevodníkom ako serverom a stunnel-om ako klientom.....	13
2.3.1 Prevodník ako server s SSL.....	13
2.3.2 Stunnel klient s SSL.....	14
3. HTTPS pre webové rozhranie prevodníka.....	16
3.1. Vypnutie nezabezpečeného protokolu HTTP.....	17
4. Konfigurácia SSL.....	19
5. Vytvorenie privátneho kľúča a samo-podpísaného certifikátu.....	21

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 prevodník správať ako server pod Tunnel > Accept Mode > Protocol, alebo ak sa má prevodník správať ako klient pod Tunnel > Host 1 > Connect Mode > Protocol.

AES Encrypt Key:	<input type="text" value="0kNYGTbyju65#%&&(9*-jHT3912768)*"/> <input checked="" type="radio"/> Text <input type="radio"/> Hexadecimal
AES Decrypt Key:	<input type="text" value="306B4E59475462796A7536352325262628392A2D6A485433"/> <input type="radio"/> Text <input checked="" type="radio"/> Hexadecimal

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 užívateľský kľúč/kľúče a musí byť nadefinovaný minimálne jeden SSH autorizovaný užívateľ. Kľúče je možné vygenerovať v prevodníku, alebo nahrat' cez webové rozhranie. Sú podporované kľúče RSA a DSA s dĺžkou 512, 768, 1024 bitov. Užívateľ musí mať zadané 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.

The screenshot displays the SSH configuration page. On the left is a sidebar with menu items: 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. The main content area is titled 'SSH Server: Host Keys' and contains several sections: 'SSH Server: Host Keys' and 'SSH Client: Known Hosts' at the top; 'SSH Server: Authorized Users' and 'SSH Client: Users' below. The 'Upload Keys' section has 'Private Key:' and 'Public Key:' fields with 'Browse...' buttons and 'No file selected.' text, and a 'Key Type:' dropdown with 'RSA' and 'DSA' options. A red 'Submit' button is present. The 'Create New Keys' section has 'Key Type:' and 'Bit Size:' (512, 768, 1024) options, also with a red 'Submit' button. The 'Current Configuration' section shows a table with 'Public RSA Key:' and 'Public DSA Key:' rows, each with 'View Key' and 'Delete Key' links. A 'Help' sidebar on the right explains that SSH Server Host Keys are used by all applications and can be created elsewhere or generated on the device. It also notes that if uploading existing keys, the Private Key must be secure. A note specifies supported key lengths: 512, 768, 1024 & 2048 bits for external SSH Certificates, and that some SSH Clients require RSA Host Keys to be at least 1024 bits in size.

SSH Server: Host Keys

SSH Client: Known Hosts

SSH Server: Authorized Users

SSH Client: Users

SSH Server: Authorized Users

Username:

Password:

Public RSA Key: Browse... No file selected.

Public DSA Key: Browse... No file selected.

Add/Edit

Help

The SSH Server Authorized Users are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CLI) and Tunneling in Accept Mode.

Every user account must have a **Password**.

The user's **Public Keys** are optional and only necessary if public key authentication is wanted. Using public key authentication will allow a connection to be made without the password being asked at that time.

Current Configuration

No Authorized Users are currently configured for the SSH Server.

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 nahráť cez webové rozhranie.


1.3. SSL

SSL je univerzálny šifrovací protokol na zabezpečenie TCP/IP komunikácie. Prevodník ho môže využiť 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 nahráť vlastný certifikát spolu s autorizačným certifikátom. Self-signed certifikát je typu RSA s dĺžkou kľúča 1024, alebo 2048 bitov.

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

SSL

Upload Certificate

New Certificate: No file selected.

New Private Key: No file selected.

Upload Authority Certificate

Authority: No file selected.

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires: mm/dd/yyyy

Key length: 1024 bit 2048 bit

Type: RSA

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.

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 blokovane. 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 **Tunnel** 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**.

- 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

Tunnel 1

Statistics	Serial Settings	Packing Mode
Accept Mode	Connect Mode	Disconnect Mode
Modem Emulation		

[Help](#)

Tunnel Accept Mode controls how a tunnel behaves when a connection attempt originates from the network.

Tunnel 1 - Accept Mode

Mode:	Always <input type="text" value="v"/>
Local Port:	<input type="text" value="10001"/>
Protocol:	TCP AES <input type="text" value="v"/>
TCP Keep Alive:	<input type="text" value="45000"/> milliseconds
AES Encrypt Key:	<input type="text" value="00112233445566778899aabbccddeeff"/> <input type="radio"/> Text <input checked="" type="radio"/> Hexadecimal
AES Decrypt Key:	<input type="text" value="00112233445566778899aabbccddeeff"/> <input type="radio"/> Text <input checked="" type="radio"/> Hexadecimal
Flush Serial:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Password:	<input type="text" value="<None>"/>
Email on Connect:	<input type="text" value="<None>"/> <input type="text" value="v"/>
Email on Disconnect:	<input type="text" value="<None>"/> <input type="text" value="v"/>
CP Output:	Group: <input type="text"/>

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. Spustíte aplikáciu Lantronix Secure Com Port Redirector.
2. Kliknete 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 Encryption**.
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**.

Secure CPR Manager 4.3.2.1

File Com Port Device Tools Help

Add/Remove Save Refresh Search For Devices Exclude

Com Ports Hide Settings Com 5 Tests

All Com Ports (2)
Com 1 - 5
Com 1 (Inaccessible)
Com 5

Com 5

Window's Port Name: Lantronix Secure CPR Port (COM5)
Window's Device Name: \Device\ScprDevice5
Window's Service Name: ScprDrv

Com Status: Closed
Network Status: Disconnected

Reset to Defaults Cancel Edits

Buffer Writes (Keep checked for better write performance)
 Server Reconnect
 No Net Close

7 Connection Timeout (in seconds)
 Timeout Reconnect 0 Reconnect Limit (0 = forever)

Listen Mode Normal - port closed after disconnect TCP Port Add To Firewall

TCP KeepAlive 7200000 KeepAlive Time (msec) 1000 KeepAlive Interval (msec)

RFC 2217 (TruPort) DTR (In): Tie DTR to DCD, DSR always active
This version of CPR does not support RFC2217 and AES to be enabled at the same time. This will be supported in a future version of CPR.

AES Encryption
Key Length 128 32 hex characters (nibbles) are needed for a key length of 128 bits.
Key Bytes

Service	Host	TCP Port
1	169.254.100.10	10001
2		
3		
4		
5		
6		
7		
8		

WARNING! If the Host is on the other side of a router or a firewall, then UDP ports 30718, 43282 and 43283 may need to be added to the firewall's exclusion list. You may experience trouble opening this com port if these UDP ports are not excluded.

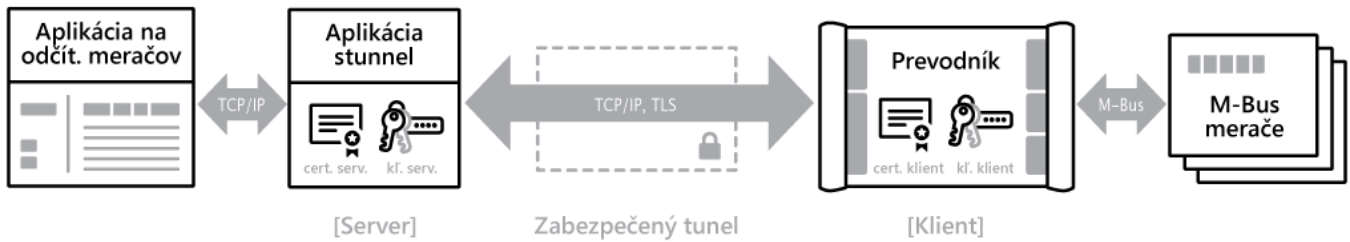
Also, some legacy device servers respond on UDP port 43283. If you are unable to connect to a device server, one possible cause is the Firewall on this machine is blocking this port. Press the 'Add Rx Port' button to add this port to the Firewall. If the button caption reads 'Remove Rx Port' then the port has already been added and can be removed by pressing this button.

Add Rx Port The Firewall is turned OFF

Device List Collapse

IP Address	# Ports	TCP Port	Product	ID	HW Address	Network Interface	Device Name	Port Name

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.

Host 1:	169.254.100.1:10001, SSL, 45000 msec
----------------	--------------------------------------

Host 1	Address:	169.254.100.1
	Port:	10001
	Protocol:	SSL
	Validate Certificate:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	TCP Keep Alive:	45000 milliseconds

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 authority.

Certifikát stunnel servera (cert_stunne1.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.



SNMP

SSH

SSL

Syslog

Custom

Upload Authority Certificate

Authority: No file selected.

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.

- 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

Tunnel 1

Statistics	Serial Settings	Packing Mode
Accept Mode	Connect Mode	Disconnect Mode
Modem Emulation		

Help

Tunnel Connect Mode controls how a tunnel behaves when a connection attempt originates locally.

For more information on **Protocol SSL**, see the [SSL](#) page.

Tunnel 1 - Connect Mode

Mode:	Always ▼
Local Port:	<input style="width: 80%;" type="text"/>
Host 1	Address: <input style="width: 80%;" type="text" value="169.254.100.1"/>
	Port: <input style="width: 80%;" type="text" value="10001"/>
	Protocol: ▼ SSL
	Validate Certificate: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	TCP Keep Alive: <input style="width: 80%;" type="text" value="45000"/> milliseconds
Host 2:	<None>
Reconnect Timer:	<input style="width: 80%;" type="text" value="1000"/> milliseconds
Flush Serial Data:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Email on Connect:	<None> ▼
Email on Disconnect:	<None> ▼
CP Output:	Group: <input style="width: 80%;" type="text"/>

Submit

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 adresy 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.

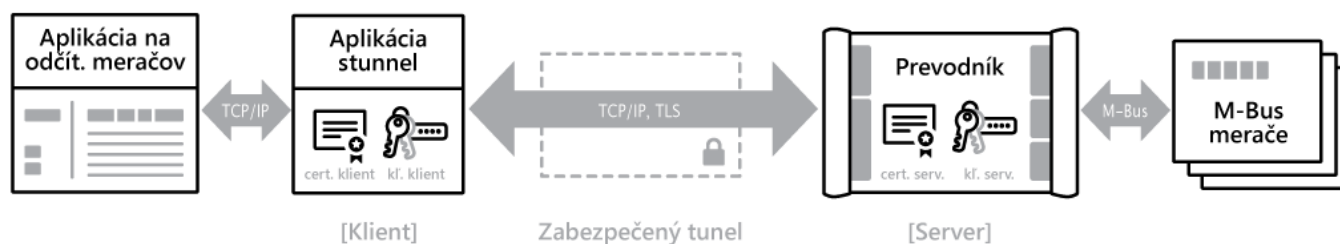
Viac informácií o možnostiach nastavenia stunnel-u nájdete tu:

<https://www.stunnel.org/static/stunnel.html>

6. V hlavnom menu stunnel-u zvolte **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**.

- 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

Tunnel 1

Accept Mode

Connect Mode

Disconnect Mode

Modem Emulation

Help

Tunnel Accept Mode controls how a tunnel behaves when a connection attempt originates from the network.

For more information on **Protocol SSL**, see the [SSL](#) page.

Tunnel 1 - Accept Mode

Mode:	Always ▼
Local Port:	10001
Protocol:	SSL ▼
TCP Keep Alive:	45000 milliseconds
Flush Serial:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Password:	<None>
Email on Connect:	<None> ▼
Email on Disconnect:	<None> ▼
CP Output:	Group: <input style="width: 100%;" type="text"/>

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 adresy 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 authority, 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 zvolte **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.

Vid' 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.

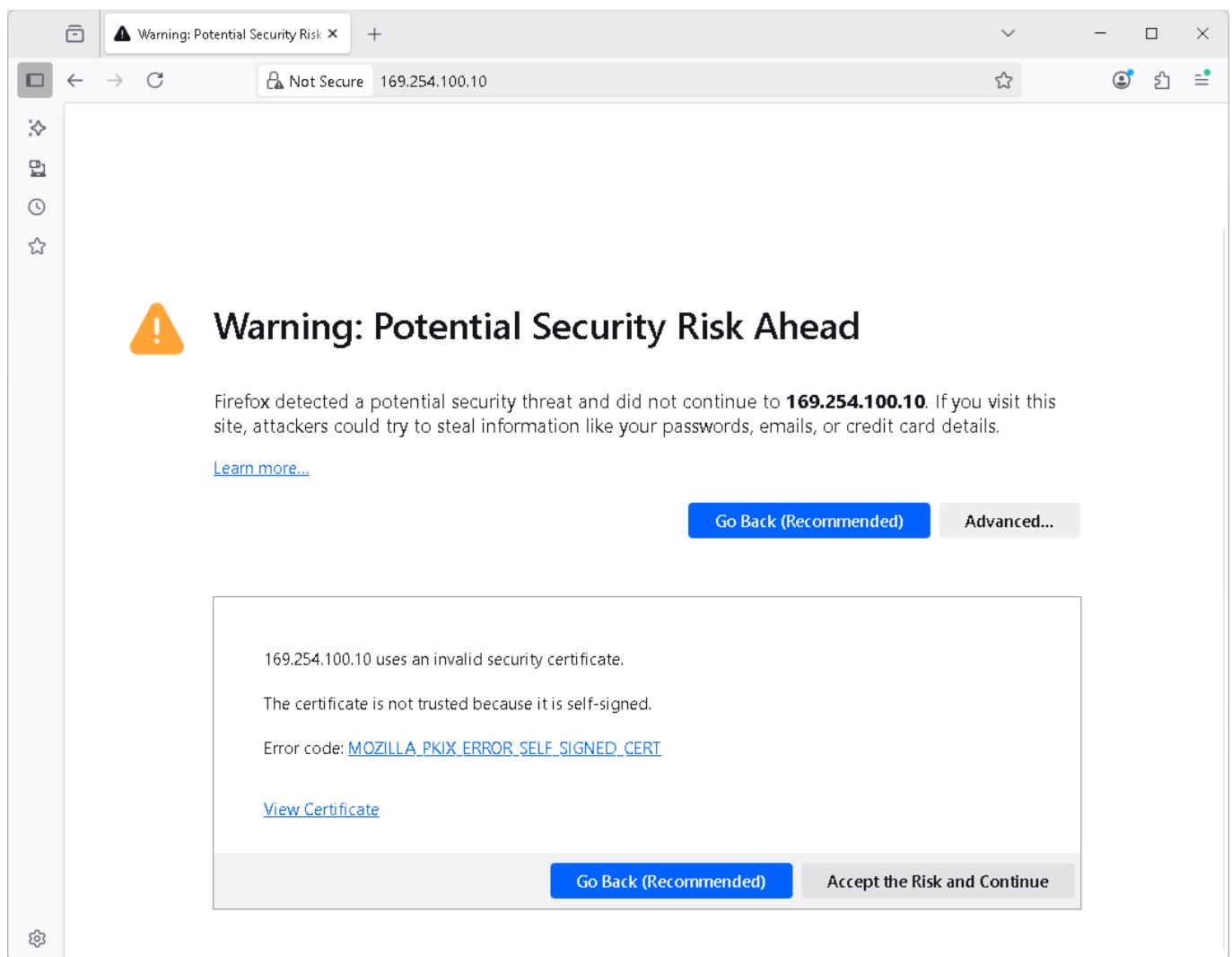
Podporované dĺžky kľúčov sú 1024, 2048 a 4096 bitov s externými certifikátmi SSL.

⚠ 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.

- 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:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Port:	<input type="text" value="0"/>	
Secure Port:	<input type="text" value="443"/>	
Secure Protocols:	<input type="checkbox"/> TLS1.0 <input type="checkbox"/> TLS1.1 <input checked="" type="checkbox"/> TLS1.2	
Max Timeout:	<input type="text" value="10"/>	seconds
Max Bytes:	<input type="text" value="40960"/>	
Logging State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Max Log Entries:	<input type="text" value="50"/>	
Log Format:	<input %b="" %r\"="" %s="" \"%{referer}i\"="" \"%{user-agent"="" type="text" value="%h %t \"/>	
Authentication Timeout:	<input type="text" value="30"/>	minutes

[Help](#)

This page displays and changes the current **HTTP Configuration** settings.

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,
Vid' 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 zvolte súbor certifikátu (`cert_converter.pem`).
5. V nastavení **New Private Key** kliknite na tlačidlo **Browse...** a zvolte súbor kľúča (`key_pkcs8_converter.pem`).
6. Kliknite na tlačidlo **Submit** v sekcii **Upload Certificate**.

- 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: No file selected.

New Private Key: No file selected.

Upload Authority Certificate

Authority: No file selected.

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires:

Key length: 1024 bit 2048 bit

Type: RSA

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.

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_Uilities

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 systému 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. Zadať 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 stunnel-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"
```