



TEKTELIC
communications
— IoT for life —

Upgrading Gateways to SNMPv3 in CLI



Introduction

- This is a reference/guide on how to enable SNMPv3, a higher security protocol, for your gateway devices
- List of Requirements:
 1. [KonaFT](#)
 2. A Command Line Program/Environment
 3. A gateway capable of SNMPv3 activation (depending on the BSP version)
 - Instructions for BSP upgrades can be found [here](#)
- The high-level procedure involves these steps:
 1. Enabling SNMPv3
 2. Verification of SNMPv3
 3. Resetting SNMPv3 Password
 4. (Optional) Re-enabling SNMPv2
 5. Logging into KonaFT

Gateway BSP Versions for SNMPv3

- Below lists the minimum BSP version for SNMPv3 activation for all TEKTELIC gateway models:
 - **Mega** – BSP 6.X.X or higher
 - **Macro** – BSP 6.X.X or higher
 - **Enterprise** – BSP 3.X.X or higher
 - **Micro** – Not supported; currently in development
 - **Micro PoE** – BSP 3.X.X or higher
 - **Micro Lite** – Not Applicable
- You can confirm the gateway's BSP version once connected in the KonaFT application:
 1. At the bottom right of the program
 2. "Board Details" tab -> "SW Management" subtab -> "Read Versions" -> "Release" version

Requirements

- [KonaFT](#)
- A program that is capable of connecting to your gateway via SSH (such as [PuTTY](#), [Tera Term](#), etc.)
- The Gateway and computer using KonaFT must be in the same subnet (in KonaFT, use *Tools -> Find My Gateway -> Scan* to determine your subnet/IP address).

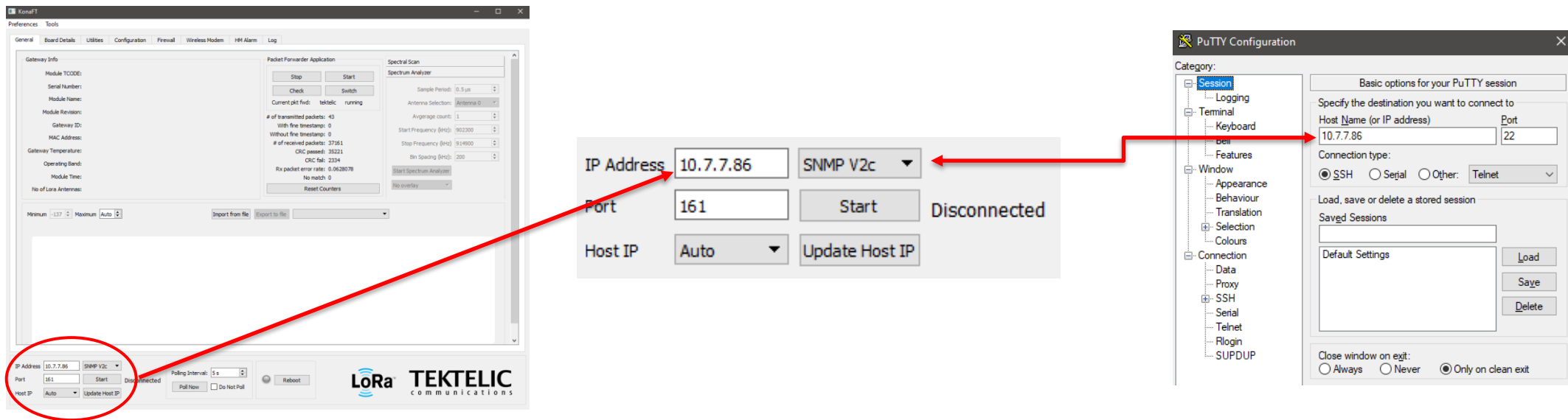


Figure-1 IP Address Configuration

Enabling SNMPv3

- Connect to your gateway through SSH. When prompted, login using the credentials below:
 - Some gateways with the “**admin**” username may still have “**root**” and the serial number as the default username and password, respectively.
- Upon logging in, you should see your gateway model and the last 6 digits of the MAC address.

Username	Password	Notes
root	9-Digit Serial Number of the gateway (i.e. 1212A3434)	• Applies to gateways with serial numbers that start with 21 and below.
admin	9-Digit Serial Number of the gateway (i.e. 1212A3434)	• Applies to gateways with serial numbers that start with 21 and below.
admin	Random string of characters provided in the test report.	• Applies to gateways with serial numbers that start with 22 and above.

Table-1 Gateway Login Credentials

Note: If the password is not on the test report, please contact [TEKTELIC Support](#) and provide the following:

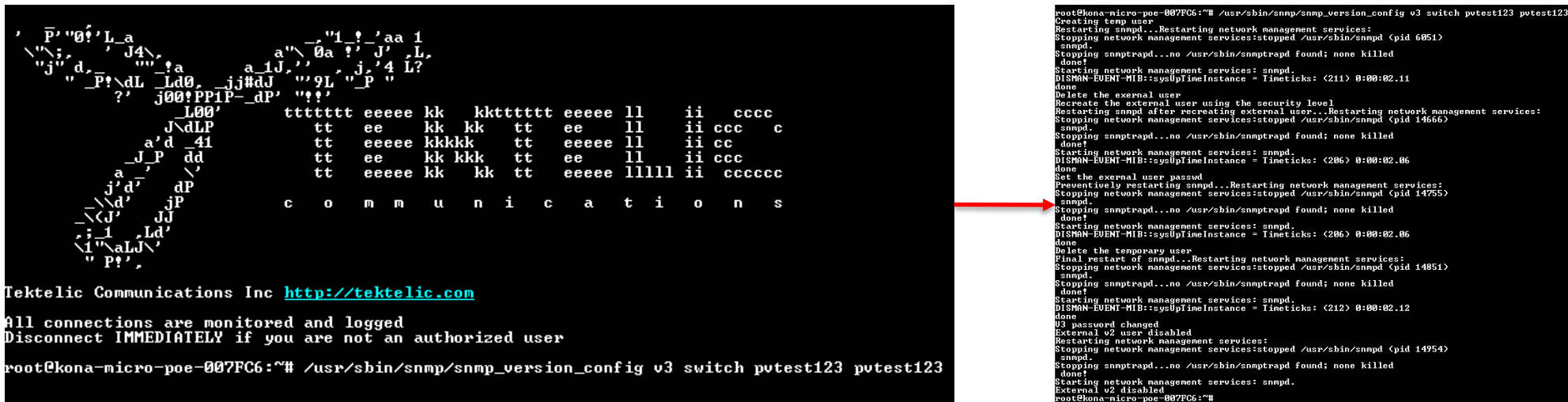
- T-code (i.e. **T000XXYY**), Revision (i.e. **A1**), and serial number (i.e. **1212A3434**)

Enabling SNMPv3 (cont.)

- Execute the following command in the SSH program to enable SNMPv3:
 - NOTE:** The password must be a minimum of 8 characters.

```
/usr/sbin/snmp/snmp_version_config v3 switch <new_password> <new_password>
```

- After executing the command, SNMPv2 will be disabled and SNMPv3 will be enabled.



```
root@kona-micro-poe-007FC6:~# /usr/sbin/snmp/snmp_version_config v3 switch pttest123 pttest123
Creating temp user
Restarting snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 6051)
snmpd.
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (211) 0:00:02.11
done
Delete the external user
Recreate the external user using the security level
Restarting snmpd after recreating external user...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 1466)
snmpd.
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (206) 0:00:02.06
done
Set the external user passwd
Preventively restarting snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 14755)
snmpd.
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (206) 0:00:02.06
done
Delete the temporary user
Final restart of snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 14951)
snmpd.
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (212) 0:00:02.12
done
U3 password changed
External v2 user disabled
Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 14954)
snmpd.
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
External v2 disabled
root@kona-micro-poe-007FC6:~#
```

Figure-2 Enabling SNMPv3 Command and Output

Verification of SNMPv3

- To confirm if SNMPv3 is active, execute the following command in the SSH program:

```
/usr/sbin/snmp/snmp_version_config v3 isenabled
```

- The output will return “**true**”.
- To confirm if SNMPv2 is inactive, execute the following command in the SSH program:

```
/usr/sbin/snmp/snmp_version_config v2 isenabled
```

- The output will return “**false**”.

```
root@kona-micro-poe-007FC6:~# /usr/sbin/snmp/snmp_version_config v3 isenabled
true
root@kona-micro-poe-007FC6:~# /usr/sbin/snmp/snmp_version_config v2 isenabled
false
root@kona-micro-poe-007FC6:~#
```

Figure-3 Verifying SNMPv3 is Enabled and SNMPv2 is Disabled

Verification of SNMPv3 (cont.)

- If you need to check the security protocol of your gateway and the encryption ID, execute the following command in the SSH program:

```
cat /etc/snmp/snmpd.d/snmpd-local.conf
```

- At the bottom of the output, the information will be displayed in a format similar to the following:

```
createUser konaPublic SHA256 0000AAAA1111BBBB AES
```

```
# Warning: the minimum pass phrase length is 8 characters.  
createUser konaPublic SHA256 AES  
root@kona-micro-poe-007FC6:~#
```

Figure-4 Example Encryption ID of SNMPv3

Resetting SNMPv3 Password

- In order to reset the password for SNMPv3, enter the following command in the SSH program:
 - **NOTE:** The password must be a minimum of 8 characters.

`/usr/sbin/snmp/snmp_version_config v3 reset <new_password> <new_password>`

```
root@kona-micro-poe-007FC6:~# /usr/sbin/snmp/snmp_version_config v3 reset newpassword newpassword
Creating temp user
Restarting snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 15047?)
snmpd
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (209) 0:00:02.09
done
Delete the external user
Recreate the external user using the security level
Restarting snmpd after recreating external user...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 20507?)
snmpd
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (206) 0:00:02.06
done
Set the external user passwd
Preventively restarting snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 20597?)
snmpd
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (205) 0:00:02.05
done
Delete the temporary user
Final restart of snmpd...Restarting network management services:
Stopping network management services:stopped /usr/sbin/snmpd (pid 20693?)
snmpd
Stopping snmptrapd...no /usr/sbin/snmptrapd found; none killed
done!
Starting network management services: snmpd.
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (210) 0:00:02.10
done
US password reset
root@kona-micro-poe-007FC6:~#
```

Figure-5 SNMPv3 Password Reset Command

(Optional) Re-enabling SNMPv2

- To reenble SNMPv2, please execute the following command:

```
/usr/sbin/snmp/snmp_version_config v2 enable
```

- To disable SNMPv2, please execute the following command:

```
/usr/sbin/snmp/snmp_version_config v2 disable
```

- **NOTE:** Both protocols can be active at the same time.

Logging into KonaFT

- Now SNMPv3 is enabled, the gateway login procedure through KonaFT will be as follows:
 - Enter the IP address for the gateway and switch to SNMPv3 in KonaFT; press Start
 - Enter konaPublic as the user name, and your newly created password (both are case sensitive); press OK to connect

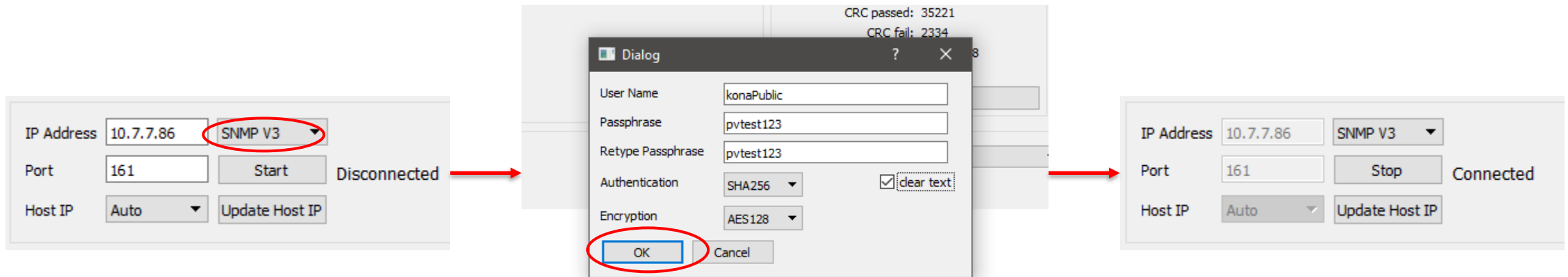


Figure-6 SNMPv3 Connection in KonaFT

Best-In-Class, Carrier Grade &
Most Cost Effective
Portfolio of Gateways, Network Server,
Sensors & Applications