TEKTELIC Communications Inc.
7657 10th Street NE Calgary, Alberta
Canada, T2E 8X2

KONA Link User Guide

Ver 1.0

Table of Contents

1. Introduction

NOTE: To have all the latest Kona Link features available make sure you're using the correct BSP or upgrade to it in section Upgrade Firmware. This document refers to the BSP v7.2.x and later.

1.1 Description

This document describes the components involved and the steps required to set up and work with a KONA Link application used for locally connected gateways. This application is the space for initial gateway setup and to read current gateway status.

KONA Link features include:
Setup wizards for easy getaway setup in different cases:

- KONA Element Set Up – for using KONA Element to manage TEKTELIC KONA Gateways.
- KONA Core Set Up – for using TEKTELIC KONA Core as your LoRaWAN Network Server.
- ChirpStack Set Up – for using ChirpStack as your LoRaWAN Network Server
- LoRa Basics Station Set Up – for using a LoRa Basics Station based Network Severs.
- Generic UDP Set Up – for use with Network Servers that use Semtech's legacy UDP interface.

Network setting capabilities:

- Network settings – set up network connection type and manage its details such as IP address type, network interface priorities and shared network access from the gateway.
- Cellular settings – manage APN profiles, configure SIM slot and modem settings.
- Firewall settings – configure firewall rules to suit your network requirements.
- OpenVPN settings – set up a secure VPN tunnel to connect gateway to remote networks.
- IPSec settings – establish a secure tunnel with IPSec for private communication.

System performance elevation features:

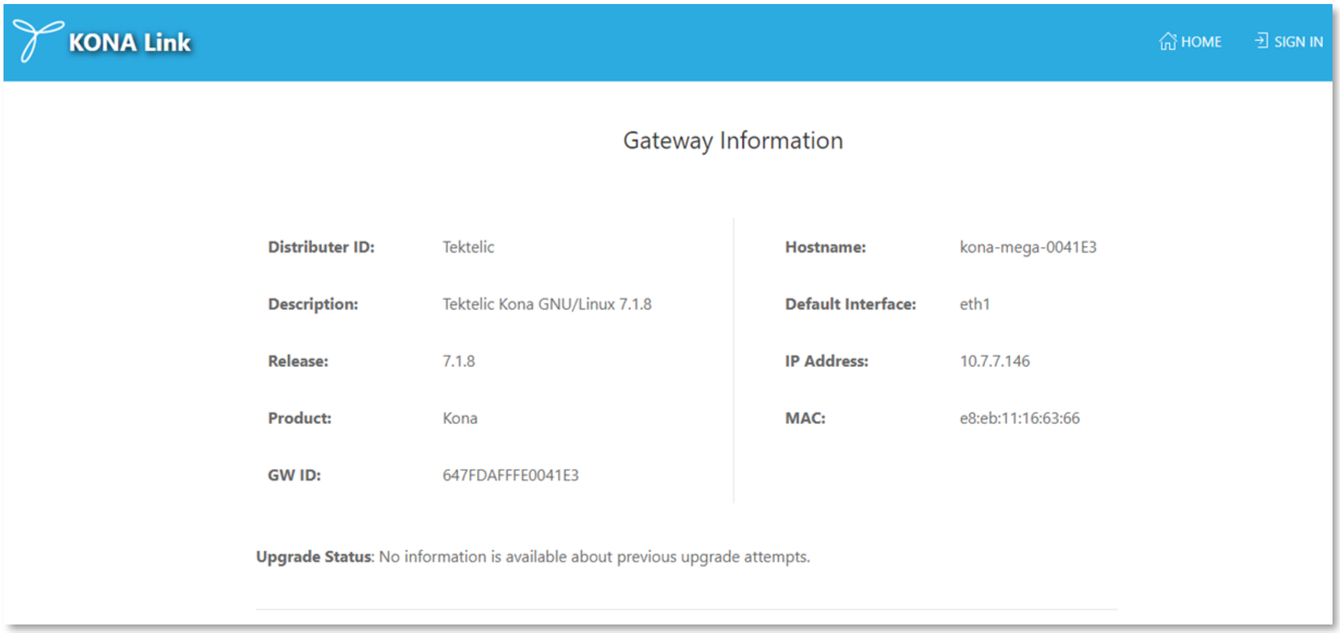
- General settings – set up gateway event reporting and other settings.
- Password management – update the login password for KONA Link.
- BSP Firmware Upgrades – Update the gateway firmware to the latest version to maintain optimal performance and security.
- Gateway Logs – view and download logs for troubleshooting or monitoring purposes.
- SNMP settings customization – set the SNMP version used on the gateway.

2. User Interface Elements

2.1 Access KONA Link

To access KONA Link:

1. Connect Gateway via Ethernet connection.
2. Make sure, that the Gateway and PC is located in same Network.
3. Open the browser.
4. Login to web page using “Host Name” or “IP Address”:
   Using “Host Name”
   Host Name URL: http://kona-<GW variant>-<last 6 digit GW ID>.local/
   Eg: http://kona-micro-0011ab.local/
   Using “IP Address”
   IP Address URL: http://<GW IP Address>/
   Eg: http:// 192.0.2.111/
5. At the main page you can review your gateway information before logging in Kona Link

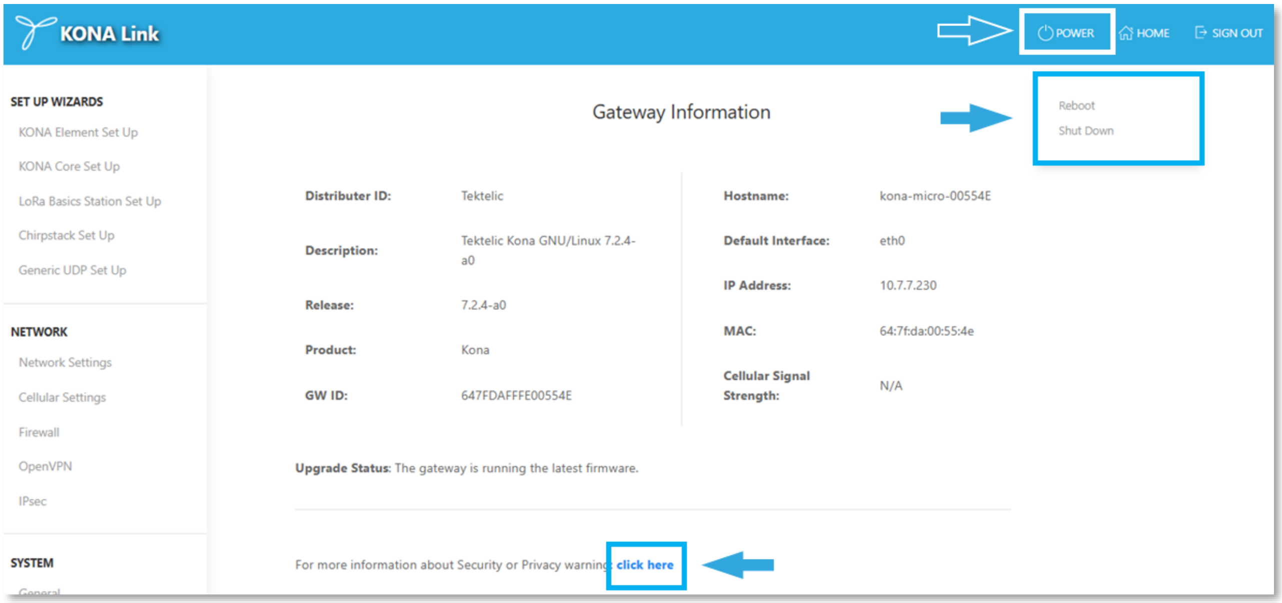


Gateway Information

Distributer ID:	Tektelic	**Hostname:**	kona-mega-0041E3
Description:	Tektelic Kona GNU/Linux 7.1.8	**Default Interface:**	eth1
Release:	7.1.8	**IP Address:**	10.7.7.146
Product:	Kona	**MAC:**	e8:eb:11:16:63:66
GW ID:	647FDAFFFE0041E3		

Upgrade Status: No information is available about previous upgrade attempts.

6. Login to application using your password provided in Test Report.



Gateway Information

Distributer ID: Tektelic

Description: Tektelic Kona GNU/Linux 7.2.4-a0

Release: 7.2.4-a0

Product: Kona

GW ID: 647FDAFFFE00554E

Hostname: kona-micro-00554E

Default Interface: eth0

IP Address: 10.7.7.230

MAC: 64:7f:da:00:55:4e

Cellular Signal Strength: N/A

Upgrade Status: The gateway is running the latest firmware.

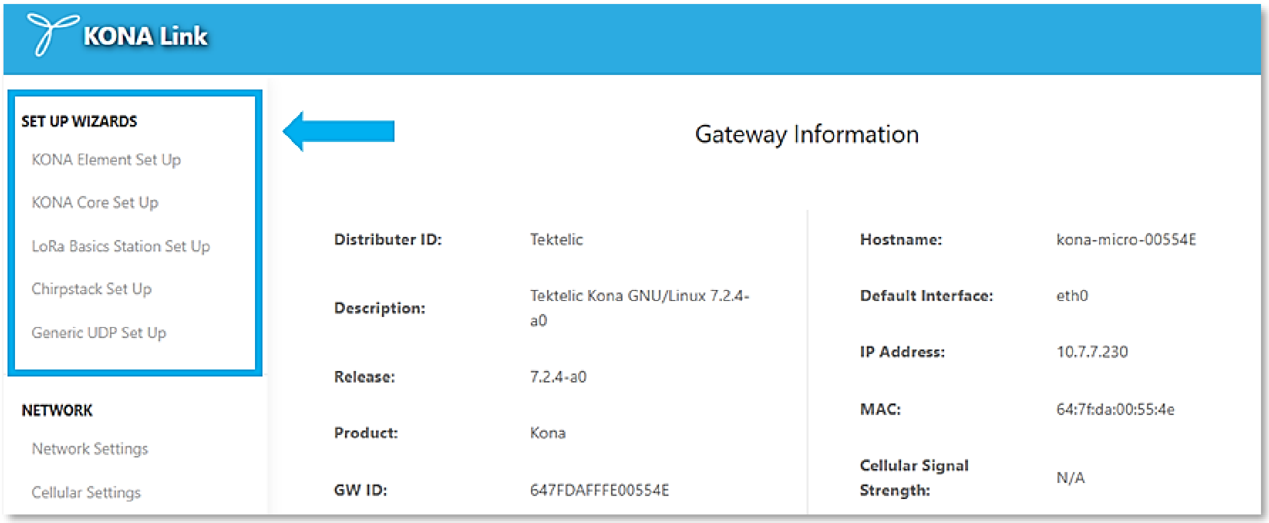
For more information about Security or Privacy warning **click here**

At the top of the main page, you can find the Power button. It allows you to reboot or shutdown gateway in case of need.

Under your Gateway information you can find the link to resolving the Security Warning issue. The KONA Gateways use a self-signed SSL certificate for security. The connection is safely encrypted, but browsers will issue a warning. You can accept this warning each time and proceed, or follow the on-screen instructions to remove this warning on your browser.

2.2 Set Up Wizards

At the main page you can and pick the Set Up Wizard that addresses your needs.



Gateway Information

Distributer ID: Tektelic

Description: Tektelic Kona GNU/Linux 7.2.4-a0

Release: 7.2.4-a0

Product: Kona

GW ID: 647FDAFFFE00554E

Hostname: kona-micro-00554E

Default Interface: eth0

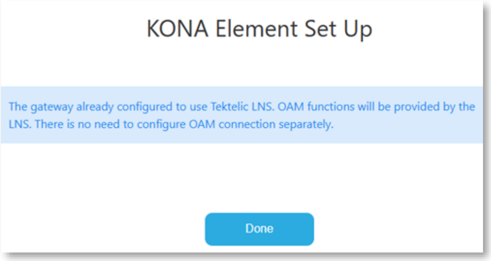
IP Address: 10.7.7.230

MAC: 64:7f:da:00:55:4e

Cellular Signal Strength: N/A

2.2.1 KONA Element Set Up

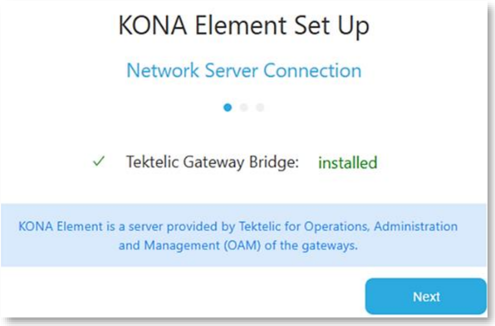
The KONA Element setup wizard configures the connection to the TEKTELIC KONA Element OA&M Server. KONA Element is used to remotely manage TEKTELIC KONA gateways, allowing them to be configured, monitored, and upgraded. You will need to have a KONA Element account to use this functionality.



KONA Element Set Up

The gateway already configured to use Tektelic LNS. OAM functions will be provided by the LNS. There is no need to configure OAM connection separately.

KONA Element can be used along with non-TEKTELIC network servers. It is not required when using the KONA Core Network Server, as KONA Core provides the same functionality for management of TEKTELIC KONA gateways.



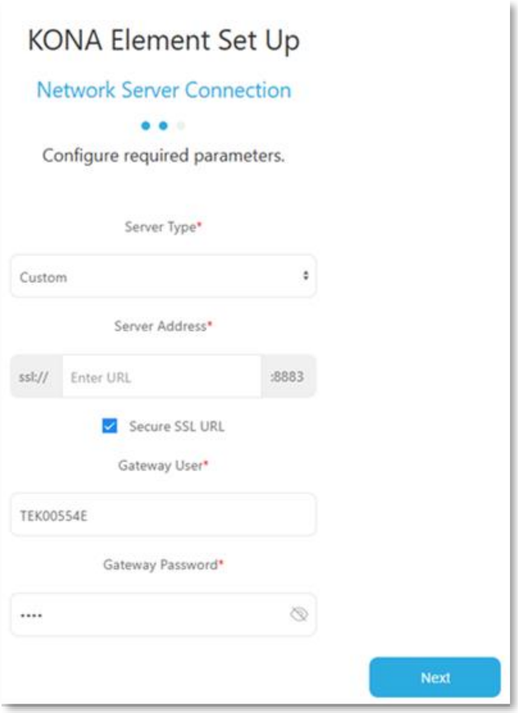
KONA Element Set Up

Network Server Connection

✓ Tektelic Gateway Bridge: installed

KONA Element is a server provided by Tektelic for Operations, Administration and Management (OAM) of the gateways.

Otherwise press “Next”.



KONA Element Set Up

Network Server Connection

Configure required parameters.

Server Type*: Custom

Server Address*: ssl:// Enter URL :8883

☑ Secure SSL URL

Gateway User*: TEK00554E

Gateway Password*: ••••

On the Set-Up page configure required parameters:

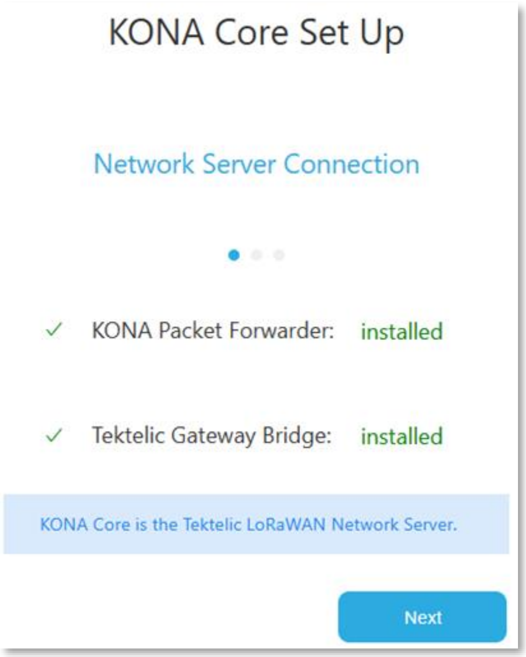
- Server type: pick cloud (North America or Europe, depending on your region) or custom (for private servers)
- Enter the server address for custom type if you have a private instance of KONA Element installed
- Optionally, set change the preconfigured gateway user name and password.
  - These must match the credentials set at the KONA Element server.

Press “Next”. After your changes will apply press “Done”.

After applying all required changes Gateway Reboot is required.

2.2.2 KONA Core Set Up

This robust KONA CORE LoRaWAN® Network Server allows end-users to remotely provision and manage their deployed Gateways and Devices while granting and protecting access to the LoRaWAN® network and providing a secure data transport from gateways to applications.



KONA Core Set Up

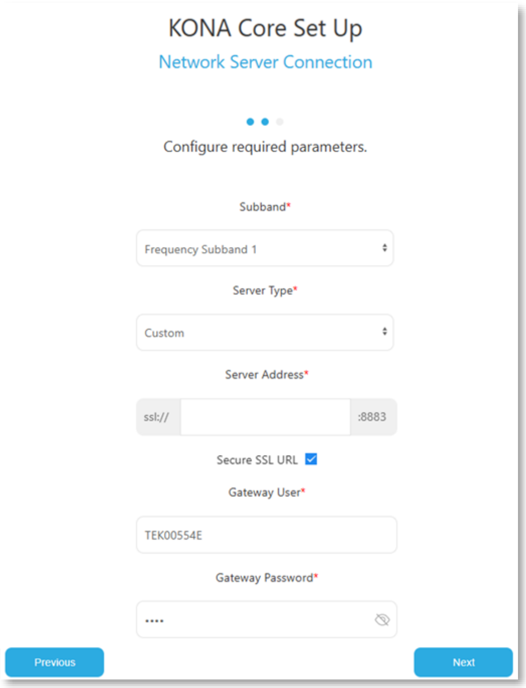
Network Server Connection

✓ KONA Packet Forwarder: installed

✓ Tektelic Gateway Bridge: installed

KONA Core is the Tektelic LoRaWAN Network Server.

KONA Core requires the KONA Packet Forwarder and Tektelic Gateway Bridge. Confirm that they are installed and press Next.



KONA Core Set Up

Network Server Connection

Configure required parameters.

Subband*: Frequency Subband 1

Server Type*: Custom

Server Address*: ssl:// :8883

Secure SSL URL ☑

Gateway User*: TEK00554E

Gateway Password*: ····

On the Set-Up page configure required parameters:

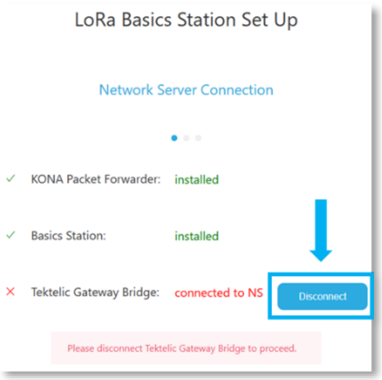
- Frequency Subband: leave the default (1) or pick based on your LNS documentation
- Server type: pick cloud (North America or Europe, depending on your region) or custom (for a private install of KONA Core)
- Enter server address if you have a custom type
- Optionally, change the preconfigured gateway user name and password.
  These must match the credentials set at the KONA Element server.

Press “Next”. After your changes will apply press “Done”.

After applying all required changes Gateway Reboot is required.

2.2.3 LoRa Basics Station Set Up

This wizard allows integration with popular third-party LoRaWAN Network servers that implement the LoRa Basics Station interface, like The Things Stack or AWS IoT Core for LoRaWAN.



LoRa Basics Station Set Up

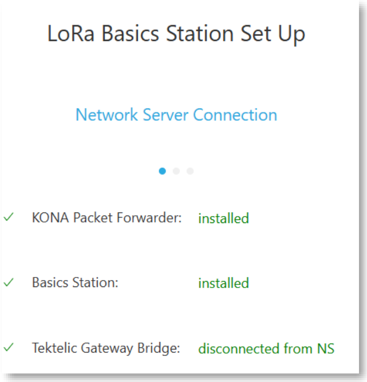
Network Server Connection

✓ KONA Packet Forwarder: installed

✓ Basics Station: installed

✕ Tektelic Gateway Bridge: connected to NS

Please disconnect Tektelic Gateway Bridge to proceed.



LoRa Basics Station Set Up

Network Server Connection

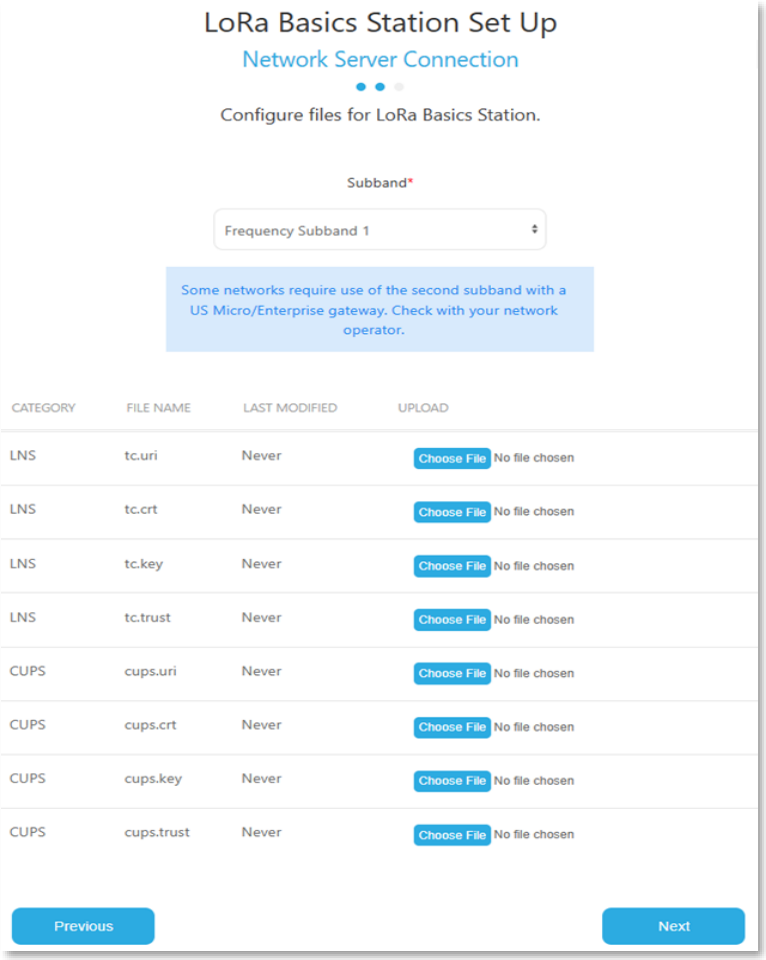
✓ KONA Packet Forwarder: installed

✓ Basics Station: installed

✓ Tektelic Gateway Bridge: disconnected from NS

To use the Basics Station interface, make sure Getaway is not connected to the KONA Core Network Server through the TEKTELIC Gateway Bridge.

Disconnect if it's not and press "Next".



LoRa Basics Station Set Up

Network Server Connection

Configure files for LoRa Basics Station.

Subband*

Frequency Subband 1

Some networks require use of the second subband with a US Micro/Enterprise gateway. Check with your network operator.

CATEGORY	FILE NAME	LAST MODIFIED	UPLOAD
LNS	tc.uri	Never	Choose File No file chosen
LNS	tc.crt	Never	Choose File No file chosen
LNS	tc.key	Never	Choose File No file chosen
LNS	tc.trust	Never	Choose File No file chosen
CUPS	cups.uri	Never	Choose File No file chosen
CUPS	cups.crt	Never	Choose File No file chosen
CUPS	cups.key	Never	Choose File No file chosen
CUPS	cups.trust	Never	Choose File No file chosen

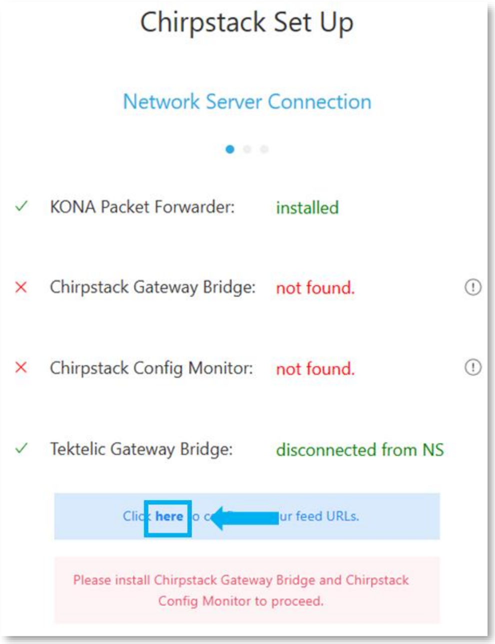
- Frequency Subband: leave the default (1) or pick based on your LNS documentation
- For the configuration files contact your LNS provider

Press "Next". After your changes will apply press "Done".

After applying all required changes Gateway Reboot is required.

2.2.4 ChirpStack Set Up

This wizard will help to integrate with a ChirpsStack network server.



Chirpstack Set Up

Network Server Connection

✓ KONA Packet Forwarder: installed

✗ Chirpstack Gateway Bridge: not found.

✗ Chirpstack Config Monitor: not found.

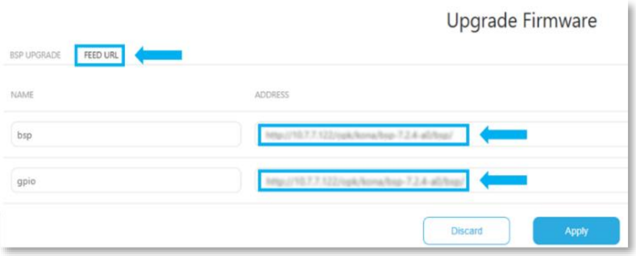
✓ Tektelic Gateway Bridge: disconnected from NS

Clic here o c ur feed URLs.

Please install Chirpstack Gateway Bridge and Chirpstack Config Monitor to proceed.

First install ChirpStack Gateway Bridge and Config Monitor.

The ChirpStack set up requires packages from ChirpStack that are not part of the standard TEKTELIC BSP. Additional feed URLs may need to be configured. Follow the provided link to configure these.

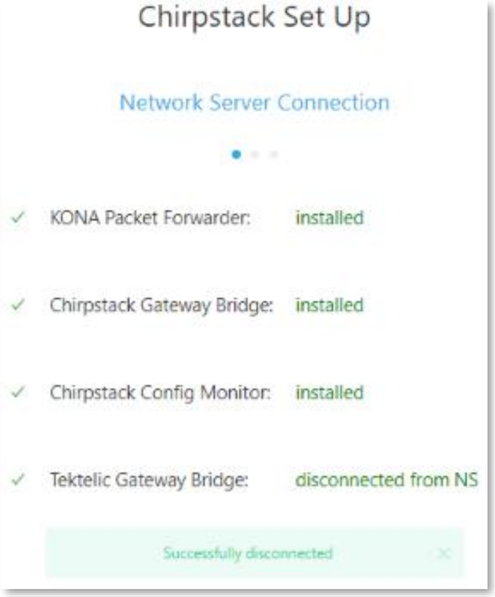


Upgrade Firmware

NAME	ADDRESS
bsp	http://10.7.7.122/opk/kona/bsp-7.2.4-a0/bsp/
gpio	http://10.7.7.122/opk/kona/bsp-7.2.4-a0/bsp/

In Upgrade Firmware menu go to FEED URL page and insert the links that will be provided by Tektelic support team with the solution.

Click “Apply”



Chirpstack Set Up

Network Server Connection

✓ KONA Packet Forwarder: installed

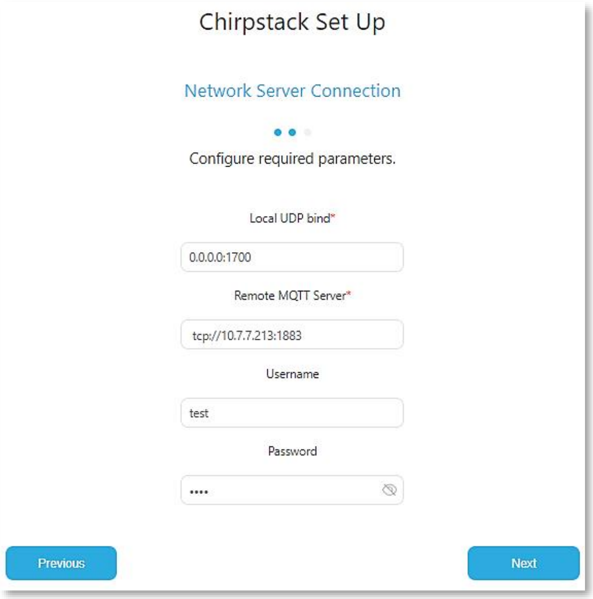
✓ Chirpstack Gateway Bridge: installed

✓ Chirpstack Config Monitor: installed

✓ Tektelic Gateway Bridge: disconnected from NS

Successfully disconnected

If the Tektelic Gateway Bridge is connected to the KONA Core Network Server, it will be disconnected to allow a connection to the ChirpStack Network Server. Once it is disconnected, press “Next”.


Chirpstack Set Up

Network Server Connection

Configure required parameters.

Local UDP bind*: 0.0.0.0:1700

Remote MQTT Server*: tcp://10.7.7.213:1883

Username: test

Password: ••••

On the Set-Up page configure required parameters:

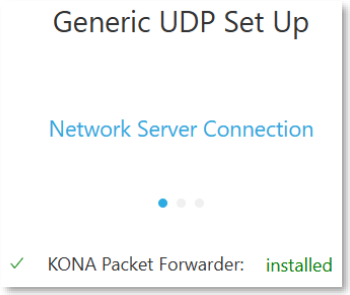
- Ensure that the Local UDP bind is set to 127.0.0.1:1700 and set the remote MQTT Server address for your ChirpStack server.
- Set the user name and password to match your ChirpStack server.

Press “Next”. After your changes will apply press “Done”.

After applying all required changes Gateway Reboot is required.

2.2.5 Generic UDP Set Up

This wizard helps to configure gateway parameters for gateways that use Semtech UDP connections.

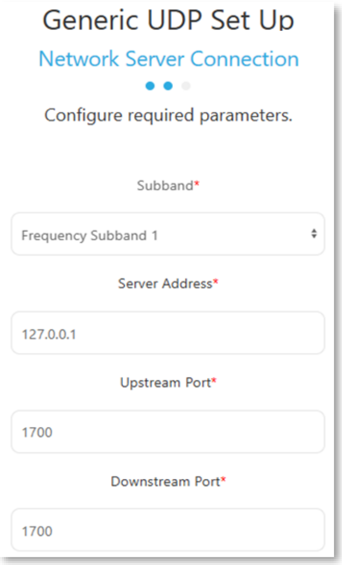

Generic UDP Set Up

Network Server Connection

✓ KONA Packet Forwarder: installed

This setup wizard will help you configure the network to handle and process generic uplink messages.

Press “Next”.


Generic UDP Set Up

Network Server Connection

Configure required parameters.

Subband*: Frequency Subband 1

Server Address*: 127.0.0.1

Upstream Port*: 1700

Downstream Port*: 1700

On the Set-Up page you can review the information from the Gateway:

- Frequency Subband: pick one of subbands based on your LNS documentation
- View Server address
- View Upstream and Downstream ports

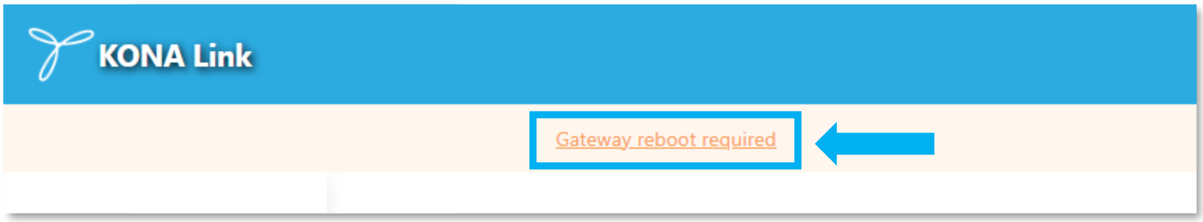
Press “Next”. After your changes will apply press “Done”.

After applying all required changes Gateway Reboot is required.

2.2.6 Gateway Reboot

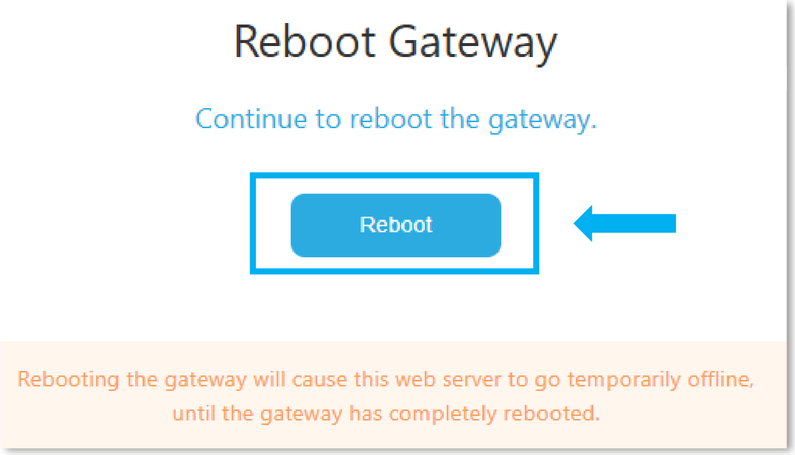
After applying Set up wizards the message that reboot is required may occur. You can proceed with other changes you need to make before rebooting gateway.

The gateway will be offline for approximately 2 minutes during the reboot. Use this to apply new settings or troubleshoot issues.



Gateway reboot required

Press it and when it transfers to the Reboot page, push “Reboot” button.

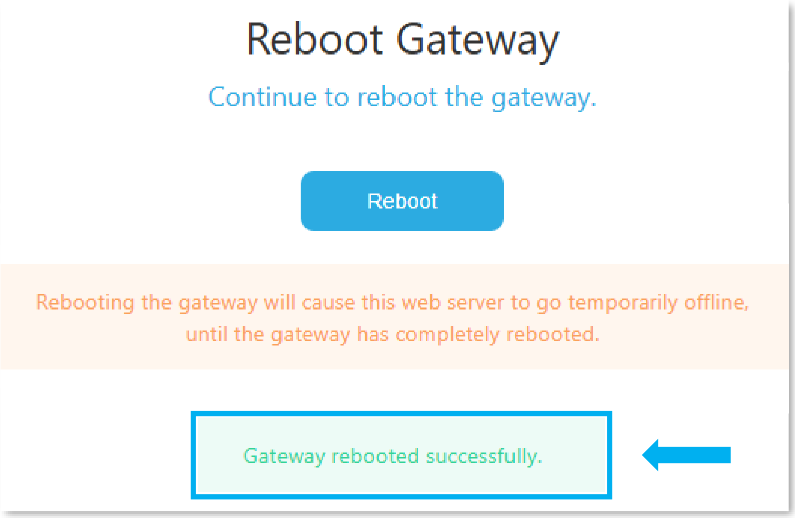


Reboot Gateway

Continue to reboot the gateway.

Rebooting the gateway will cause this web server to go temporarily offline, until the gateway has completely rebooted.

After a short period of time, you’ll see message that Gateway successfully rebooted.



Reboot Gateway

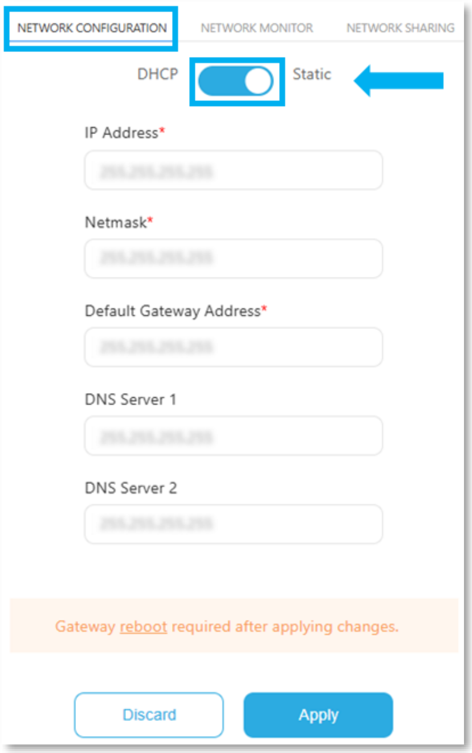
Continue to reboot the gateway.

Rebooting the gateway will cause this web server to go temporarily offline, until the gateway has completely rebooted.

Gateway rebooted successfully.

3.Network

3.1 Network Settings



IP Address*
[redacted]

Netmask*
[redacted]

Default Gateway Address*
[redacted]

DNS Server 1
[redacted]

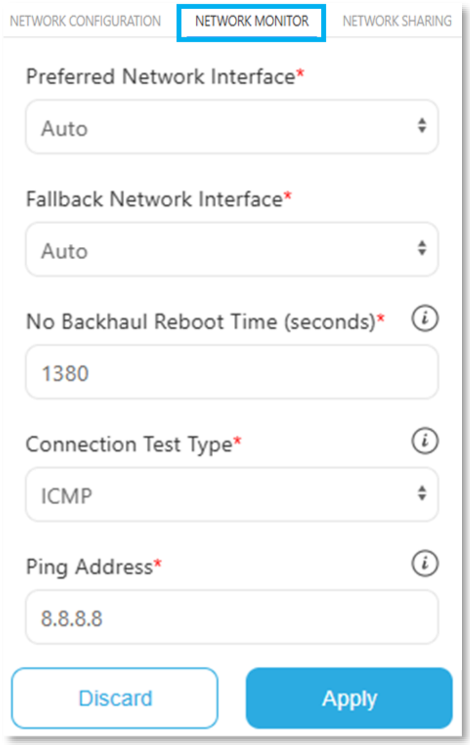
DNS Server 2
[redacted]

Gateway reboot required after applying changes.

By default, the gateway is configured for DHCP. On this page you can switch from dynamic to static IP.

To achieve that change the switch to Static, enter desired IP address, Netmask and Default Getaway address.

Press "Apply"



Preferred Network Interface*
Auto

Fallback Network Interface*
Auto

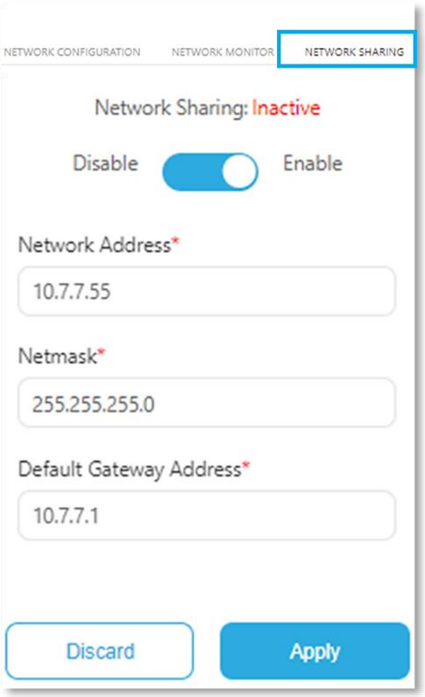
No Backhaul Reboot Time (seconds)*
1380

Connection Test Type*
ICMP

Ping Address*
8.8.8.8

To configure your getaway's network failover options on a Network Monitor page you can configure:

- Preferred Network Interface - Preferred channel to connect to network (if gateway allows more than one)
- Fallback Network Interface - The channel your gateway must use in case preferred one doesn't work properly
- No Backhaul Reboot Time (seconds) – If no interface is available after this time, the Gateway will reboot
- Connection Test Type – By default the connection is tested using ICMP Ping to a well-known server If ICMP is not supported in your network, then a TCP connection can be used.
- Ping Address – address for a connection test used. By default, this is the Google DNS server at 8.8.8.8.



Network Sharing: Inactive

Disable ● Enable

Network Address*: 10.7.7.55

Netmask*: 255.255.255.0

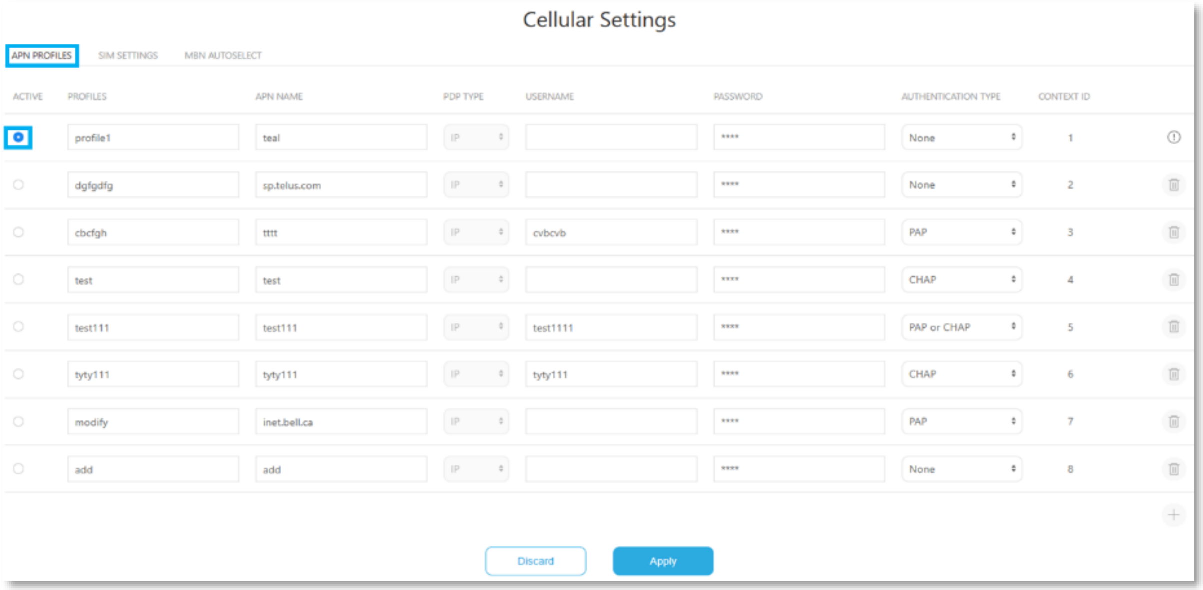
Default Gateway Address*: 10.7.7.1

Network sharing allows traffic to be routed between Ethernet and cellular network interfaces. To activate your getaway's Network Sharing go to corresponding page and switch status to "Enable".

To achieve that enter desired IP address, Netmask and Default Getaway address.

Press "Apply"

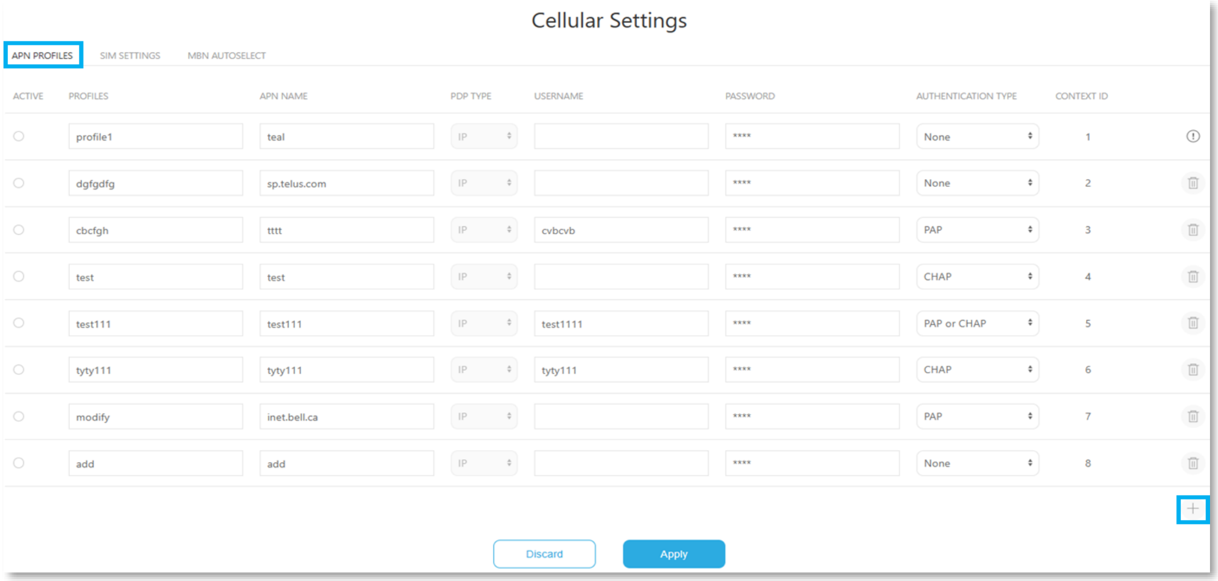
3.2 Cellular Settings



Cellular Settings

ACTIVE	PROFILES	APN NAME	PDP TYPE	USERNAME	PASSWORD	AUTHENTICATION TYPE	CONTEXT ID
●	profile1	teal	IP		****	None	1
○	dgfgdfg	sp.telus.com	IP		****	None	2
○	cbcfgh	tttt	IP	cvbcvb	****	PAP	3
○	test	test	IP		****	CHAP	4
○	test111	test111	IP	test1111	****	PAP or CHAP	5
○	tyty111	tyty111	IP	tyty111	****	CHAP	6
○	modify	inet.bell.ca	IP		****	PAP	7
○	add	add	IP		****	None	8

Activate APN: mark it in Active column and press "Apply"



Cellular Settings

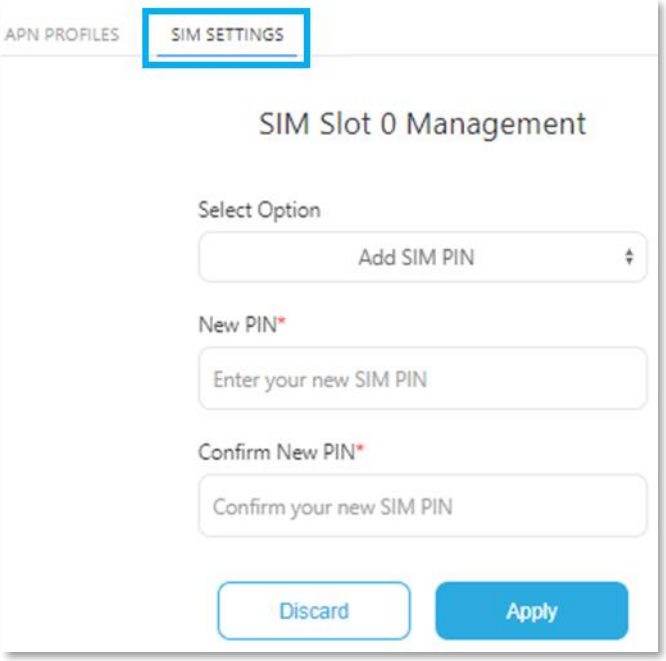
APN PROFILES | SIM SETTINGS | MBN AUTOSELECT

ACTIVE	PROFILES	APN NAME	PDP TYPE	USERNAME	PASSWORD	AUTHENTICATION TYPE	CONTEXT ID	
○	profile1	teal	IP		****	None	1	ⓘ
○	dgfgdfg	sp.telus.com	IP		****	None	2	🗑
○	cbcfgh	tttt	IP	cvbcvb	****	PAP	3	🗑
○	test	test	IP		****	CHAP	4	🗑
○	test111	test111	IP	test1111	****	PAP or CHAP	5	🗑
○	tyty111	tyty111	IP	tyty111	****	CHAP	6	🗑
○	modify	inet.bell.ca	IP		****	PAP	7	🗑
○	add	add	IP		****	None	8	🗑

Create new APN: press + button at the bottom of the table and fill the boxes with information provided by your APN provider. In case APN doesn't have username and password, put Authentication type as "None".

In case you're using AT&T or Verizon providers, please contact Tektelic customer support.

Mark it in Active column and press Apply.



SIM Slot 0 Management

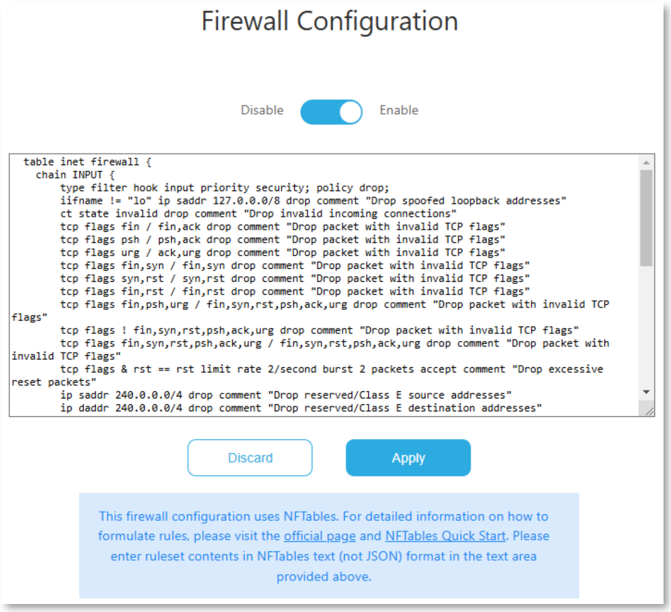
Select Option: Add SIM PIN

New PIN*: Enter your new SIM PIN

Confirm New PIN*: Confirm your new SIM PIN

In Sim Settings page you can add or edit your current SIM PIN.

3.3 Firewall



Firewall Configuration

```
 table inet firewall {
   chain INPUT {
       type filter hook input priority security; policy drop;
       iifname != "lo" ip saddr 127.0.0.0/8 drop comment "Drop spoofed loopback addresses"
       ct state invalid drop comment "Drop invalid incoming connections"
       tcp flags fin / fin,ack drop comment "Drop packet with invalid TCP flags"
       tcp flags psh / psh,ack drop comment "Drop packet with invalid TCP flags"
       tcp flags urg / ack,urg drop comment "Drop packet with invalid TCP flags"
       tcp flags fin,syn / fin,syn drop comment "Drop packet with invalid TCP flags"
       tcp flags syn,rst / syn,rst drop comment "Drop packet with invalid TCP flags"
       tcp flags fin,rst / fin,rst drop comment "Drop packet with invalid TCP flags"
       tcp flags fin,psh,urg / fin,syn,rst,psh,ack,urg drop comment "Drop packet with invalid TCP
flags"
       tcp flags ! fin,syn,rst,psh,ack,urg drop comment "Drop packet with invalid TCP flags"
       tcp flags fin,syn,rst,psh,ack,urg / fin,syn,rst,psh,ack,urg drop comment "Drop packet with
invalid TCP flags"
       tcp flags & rst == rst limit rate 2/second burst 2 packets accept comment "Drop excessive
reset packets"
       ip saddr 240.0.0.0/4 drop comment "Drop reserved/Class E source addresses"
       ip daddr 240.0.0.0/4 drop comment "Drop reserved/Class E destination addresses"
```

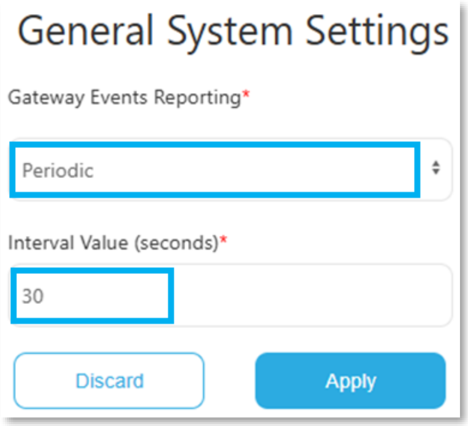
This firewall configuration uses NFTables. For detailed information on how to formulate rules, please visit the official page and NFTables Quick Start. Please enter ruleset contents in NFTables text (not JSON) format in the text area provided above.

It is recommended to keep Firewall enabled for enhanced security and protection from unauthorized access or data interception. Temporarily disabling Firewall may be useful during the setup or testing for easier communication and to avoid blocking some of the necessary traffic.

For instructions on Firewall configuration please follow links provided in the blue box.

4.System

4.1 General



General System Settings

Gateway Events Reporting*

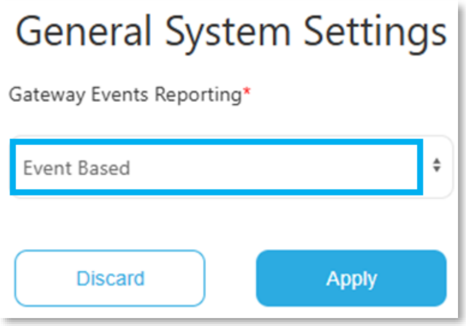
Periodic

Interval Value (seconds)*

30

You can configure how often your gateway will report events to the Network Sever.

Set periodic reporting to receive updates every set number of seconds or event-based reporting to only receive update in case gateway has any new alarms or faults.



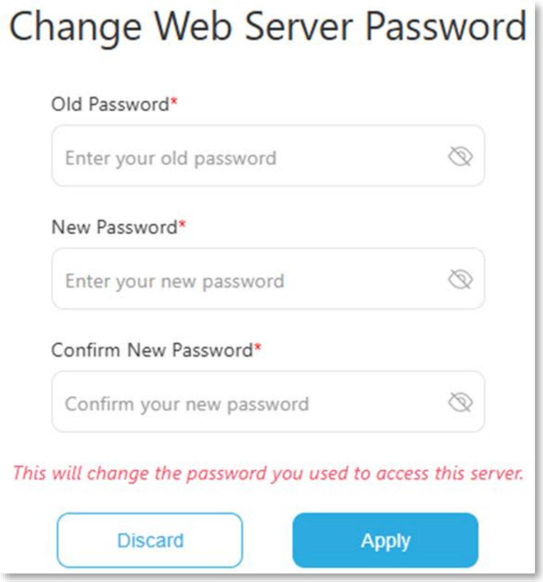
General System Settings

Gateway Events Reporting*

Event Based

This feature reduces the amount of traffic on the backhaul interface used and may be helpful where cellular data is limited.

4.2 Change Password



Change Web Server Password

Old Password*

Enter your old password

New Password*

Enter your new password

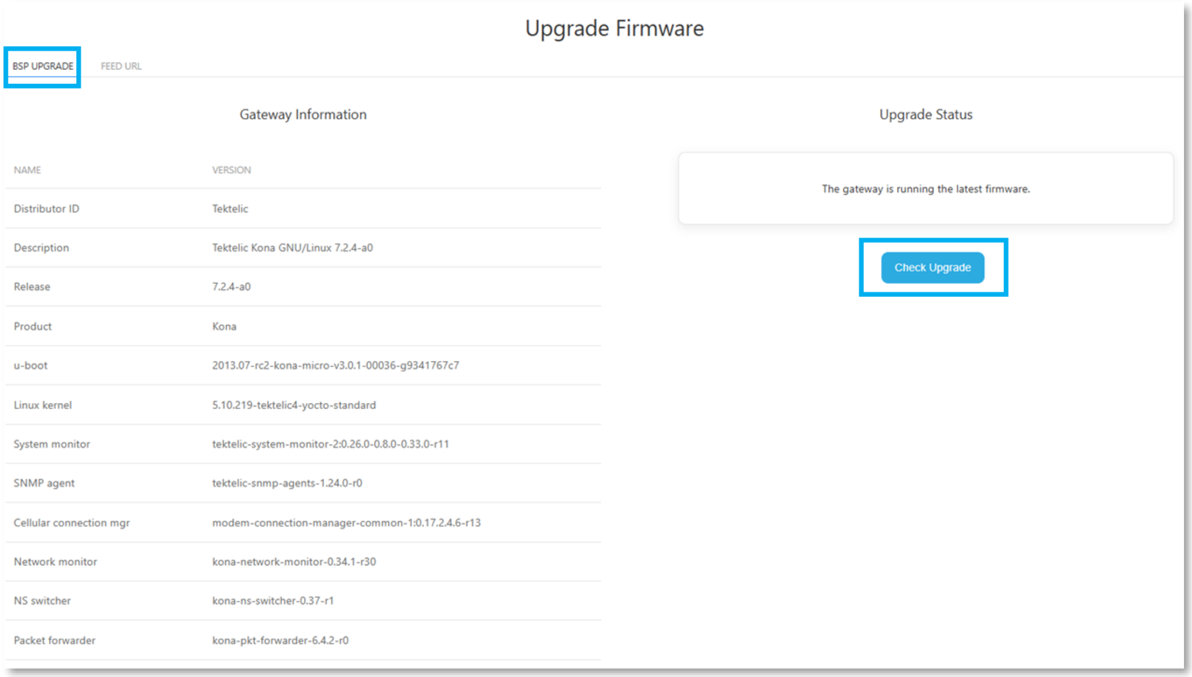
Confirm New Password*

Confirm your new password

This will change the password you used to access this server.

The default password to access KONA Link is provided on the Test Report that is included with the gateway. You can change it anytime.

4.3 Upgrade Firmware



Upgrade Firmware

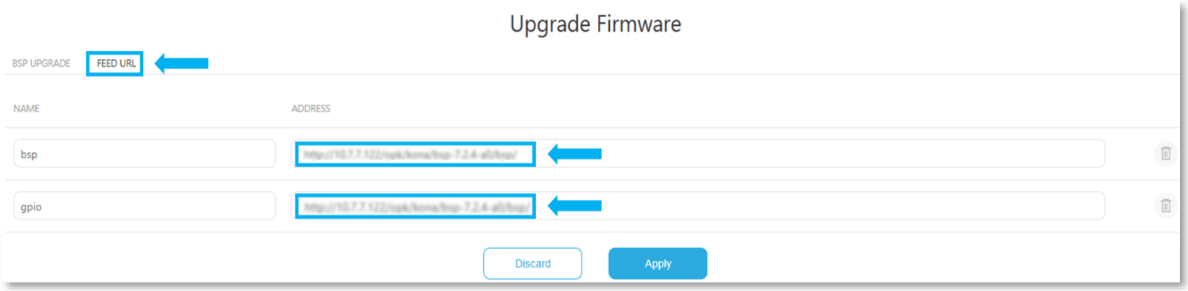
Gateway Information

NAME	VERSION
Distributor ID	Tektelic
Description	Tektelic Kona GNU/Linux 7.2.4-a0
Release	7.2.4-a0
Product	Kona
u-boot	2013.07-rc2-kona-micro-v3.0.1-00036-g9341767c7
Linux kernel	5.10.219-tektelic4-yocto-standard
System monitor	tektelic-system-monitor-2:0.26.0-0.8.0-0.33.0-r11
SNMP agent	tektelic-snmp-agents-1.24.0-r0
Cellular connection mgr	modem-connection-manager-common-1:0.17.2.4.6-r13
Network monitor	kona-network-monitor-0.34.1-r30
NS switcher	kona-ns-switcher-0.37-r1
Packet forwarder	kona-pkt-forwarder-6.4.2-r0

Upgrade Status

The gateway is running the latest firmware.

On BSP Upgrade page you can see all Gateway information and also check if there is possible firmware upgrade and apply it if needed.



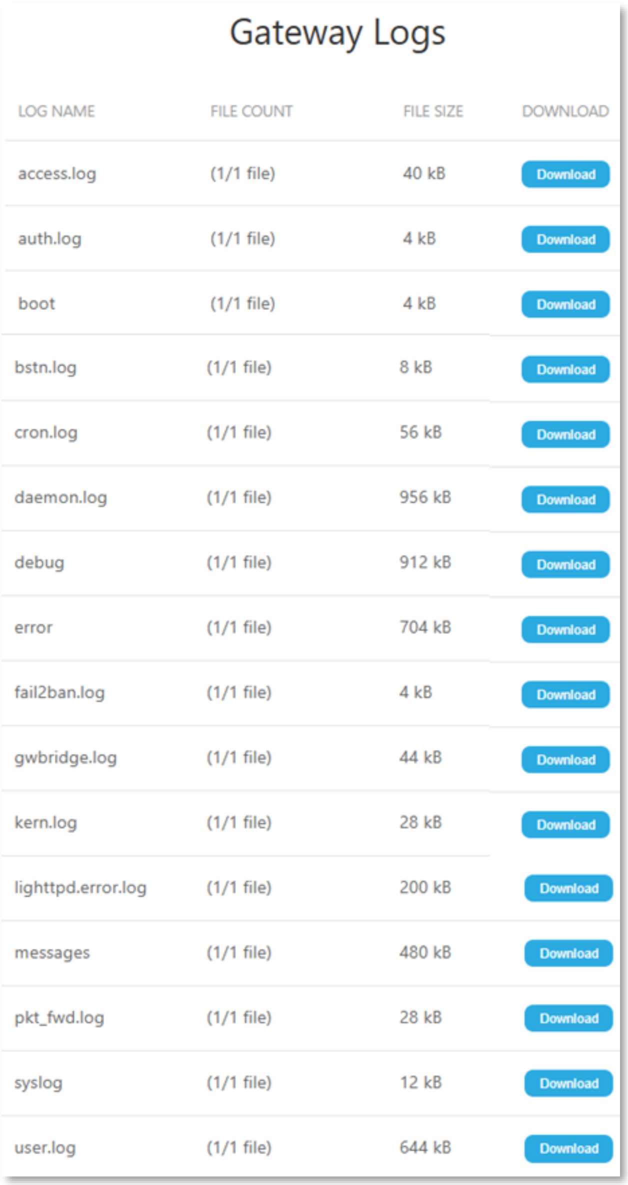
Upgrade Firmware

NAME	ADDRESS
bsp	[redacted]
gpio	[redacted]

On FEED URL page you can by inserting the links that will be provided by Tektelic customer support with the solution.

5. Advanced Configurations

5.1 Gateway Logs

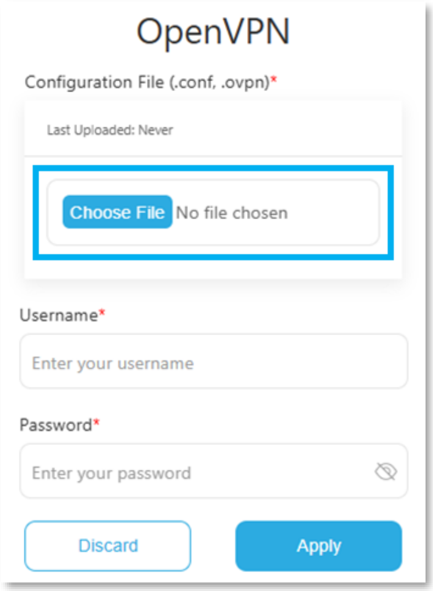


Gateway Logs

LOG NAME	FILE COUNT	FILE SIZE	DOWNLOAD
access.log	(1/1 file)	40 kB	Download
auth.log	(1/1 file)	4 kB	Download
boot	(1/1 file)	4 kB	Download
bstn.log	(1/1 file)	8 kB	Download
cron.log	(1/1 file)	56 kB	Download
daemon.log	(1/1 file)	956 kB	Download
debug	(1/1 file)	912 kB	Download
error	(1/1 file)	704 kB	Download
fail2ban.log	(1/1 file)	4 kB	Download
gwbridge.log	(1/1 file)	44 kB	Download
kern.log	(1/1 file)	28 kB	Download
lighttpd.error.log	(1/1 file)	200 kB	Download
messages	(1/1 file)	480 kB	Download
pkt_fwd.log	(1/1 file)	28 kB	Download
syslog	(1/1 file)	12 kB	Download
user.log	(1/1 file)	644 kB	Download

You can download Gateway logs in txt format for troubleshooting purposes.

5.2 Open VPN



OpenVPN

Configuration File (.conf, .ovpn)*

Last Uploaded: Never

Choose File No file chosen

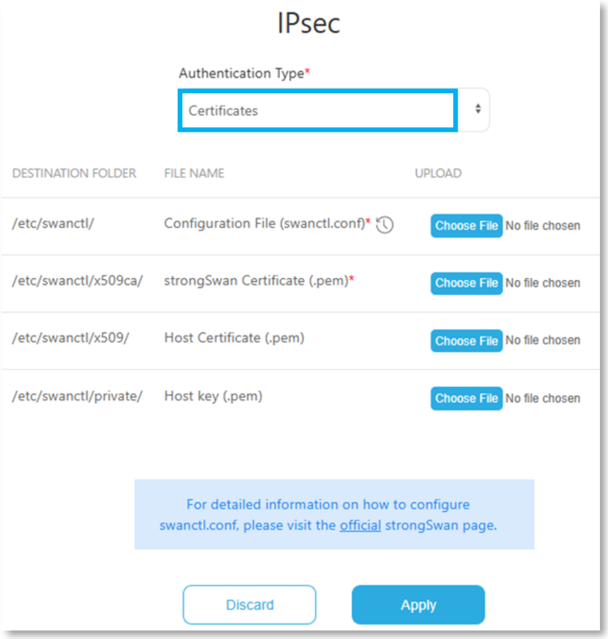
Username*

Password*

To create and configure OpenVPN:

1. Upload the OpenVPN configuration file provided by your system administrator.
2. Enter your VPN account Username and Password.
3. Press “Apply”

5.3 IPsec

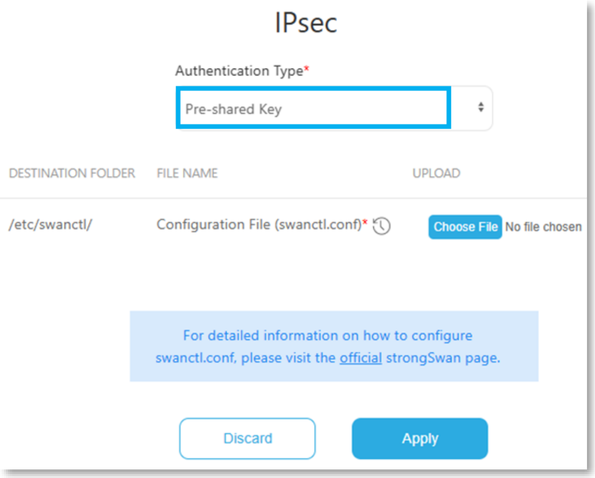


IPsec

Authentication Type*: Certificates

DESTINATION FOLDER	FILE NAME	UPLOAD
/etc/swanctl/	Configuration File (swanctl.conf)*	Choose File No file chosen
/etc/swanctl/x509ca/	strongSwan Certificate (.pem)*	Choose File No file chosen
/etc/swanctl/x509/	Host Certificate (.pem)	Choose File No file chosen
/etc/swanctl/private/	Host key (.pem)	Choose File No file chosen

For detailed information on how to configure swanctl.conf, please visit the official strongSwan page.



IPsec

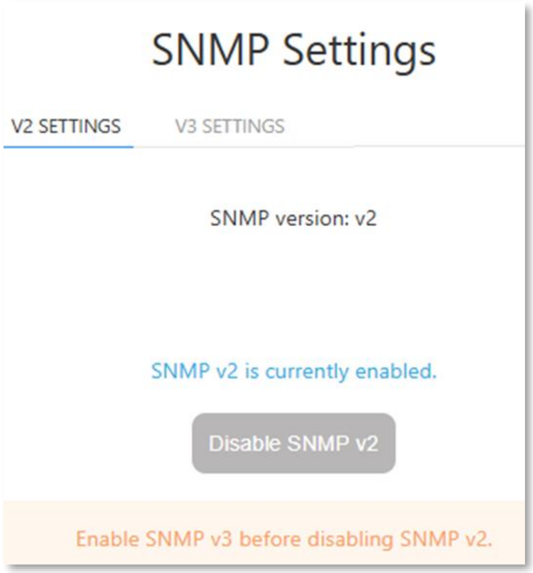
Authentication Type*: Pre-shared Key

DESTINATION FOLDER	FILE NAME	UPLOAD
/etc/swanctl/	Configuration File (swanctl.conf)*	Choose File No file chosen

For detailed information on how to configure swanctl.conf, please visit the official strongSwan page.

To configure IPsec, upload the configuration files provided by your system administrator. If required for your configuration, enter the pre-shared key.

5.4 SNMP Settings



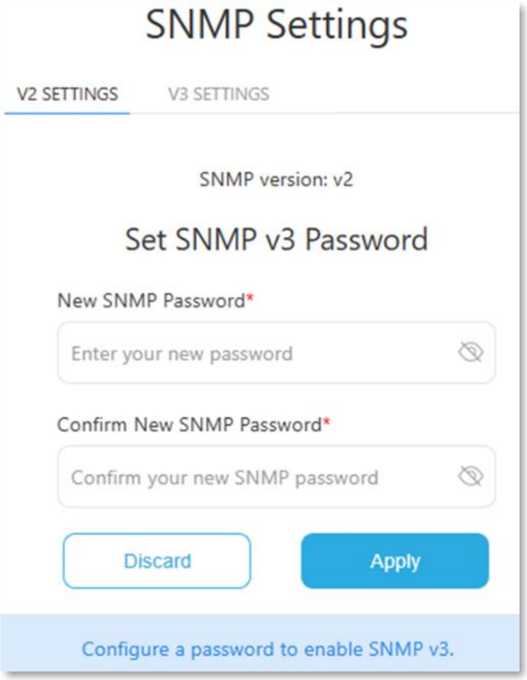
SNMP Settings

SNMP version: v2

SNMP v2 is currently enabled.

Enable SNMP v3 before disabling SNMP v2.

SNMPv2 may be enabled on your Gateways.
SNMPv3 can be used for higher security.



SNMP Settings

SNMP version: v2

Set SNMP v3 Password

New SNMP Password*

Enter your new password

Confirm New SNMP Password*

Confirm your new SNMP password

Configure a password to enable SNMP v3.

When switching from SNMPv2 to SNMPv3,
you must configure a new password.