Template:Security guidelines

□

Contents

Summary

In this article you can find details about all Teltonika's supported security features also what device has which security implementations and a guide how to use them properly.

General security guidelines

Below you may find some of the most common security recommendations - these recommendations can and should be applied not only to Teltonika devices, but to all internet-facing appliances. It is always advised to adhere to the following security recommendations whenever device is exposed to the internet in some way.

- Do not have Public Access (HTTP(S)/SSH/Telnet/CLI ports) open *without any restrictions*
- Set strong WebUI/SSH password, including numbers, lowercase and uppercase alphabet letters, symbols. Longer password length also increases overall security of the device
- If public access is necessary, have it firewalled for **specific source IPs and source ports**
- If public access is absolutely mandatory and source IPs cannot be specified for any reason, **set unconventional listening and destination ports** for any common service (i.e., set HTTP(S) port to a random number in the range of 32768-65535)
- If remote access is required – always **try to employ the usage of secure VPN protocols** instead of exposing sensitive services directly to all of the internet
- When configuring VPNs purely for security, opt in to use VPN protocols with TLS (certificate-based) or private/public key-based authentication, such as IPsec, OpenVPN, WireGuard
- **Disable WiFi if unused**. Use strong WiFi authentication otherwise (certificate based auth/strong PSK).
- When using router as a public WiFi hotspot, always make sure to restrict access from public WiFi network to the router (create a separate zone with INPUT=DROP default rule for public WiFi network, then configure specific allowed ports only if absolutely necessary)
- Make sure to provide the least amount of required permissions for any additionally created

user account
- Do not install extra packages from **unknown sources**
- **Always write down & compare MD5/SHA hashes of backup files** before uploading them back into the router. In addition – always make sure to verify the hashes of firmware files, before uploading them to the router
- Make sure to use key-based authentication wherever possible (i.e., accessing to the router via SSH)
- Set **SMS limits, data limits** for your SIM card plans
- Disable SMS utilities entirely, *if it is not utilized whatsoever*

Please note that regardless of currently running configuration, **we strongly recommend to keep up with the latest firmware version** which generally includes not only overall improvements to the router functionality, but also security patches & vulnerability fixes.

Understandably, every production environment is different and some features may be altered or changed in newer firmware versions – please always make sure to test & verify newer firmware versions **before deploying any such firmware onto devices in production environment**.

Security features

In the table below you can find all the security features supported by Teltonika's devices.

Security measurement type	Security measurement name	By default	Details
DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
	Remote ICMP Requests	On	An Internet Control Message Protocol (ICMP) flood attack, also known as a Ping flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
	SSH Attack Prevention	Off	A Secure Shell (SSH) flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with SSH requests.
	HTTP Attack Prevention	Off	A Hypertext Transfer Protocol (HTTP) flood attack is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with HTTP requests.
	HTTPS Attack Prevention	Off	Hypertext Transfer Protocol Secure (HTTPS) flood attack is same as HTTP flood attack but using HTTPS protocol instead of simple HTTP
Port Scan Prevention	Port Scan	Off	A port scan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port.
	SYN-FIN attack	Off	An attacker may send TCP/IP packets with the SYN and FIN TCP/IP flags set to a target system, ranging across all ports, to find open TCP/IP ports for further attacks. The target system will drop packets which are destined to open ports and send back RST/ACK packets for closed ports. The attacker may gather information from the system responses.
	SYN-RST attack	Off	SYN-RST attack, also known as TCP reset attack, is an abrupt closure of the session which causes the resources allocated to the connection to be immediately released and all other information about the connection is erased. TCP reset is identified by the RESET flag in the TCP header.
	X-Mas attack	Off	Christmas Tree (X-Mas) Attack is designed to send a very specifically crafted TCP packet to a device on the network. This crafting of the packet is one that turns on a bunch of flags. There is some space set up in the TCP header, called flags. And these flags all are turned on or turned off, depending on what the packet is doing.
	FIN scan	Off	FIN packets can bypass firewalls without modification. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP.
	NULLflags attack	Off	A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags. In a production environment, there will never be a TCP packet that doesn't contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and routers that filter incoming packets with particular flags.

Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Block Unwanted Access	SSH Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block SSH access from that source.
	WebUI Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block WebUI access from that source.
Configuration via SMS	SMS Utilities	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Plug and Play	UPnP	Not installed / Off	UPnP doesn't require any sort of authentication from the user. Any application running on your computer in LAN can ask the router to forward a port over UPnP, which is why the malware can abuse UPnP. Recommendation - If you don’t use it when leave it not installed or turned off.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

Security recommendations

Security features will not help if you won't use them properly, below you can find a table with recommendations.

Topic	Recommendation	Comment
SSH access	Use a different port than 22	22 is the default port used by SSH protocol. You should not use the default port as it is easy to guess and more vulnerable to brute-force attacks.
	Use strong passwords and passphrases	Most of the servers security are compromised because of the weak passwords. They use easy to guess passwords like the brand name of the device or some universal password like 123456 or Admin123. Weak password is more likely to be cracked by brute-force attacks. You should be using a very strong password or passphrase to log in your SSH server.
Firewall	Block traffic by default	Start blocking all traffic by default and only allow specific traffic to identified services. This approach provides quality control over the traffic and decreases the possibility of a breach. This behavior can be achieved by configuring the last rule in an access control list to deny all traffic.
	Reviewing firewall rules	Networks are constantly changing by gaining new users and new devices. New services and new applications are being accessed which means new firewall rules will need to be added. The old firewall rules will need to be reviewed and deleted if necessary.
VPN	Always use VPN if you have the possibility	Encrypted traffic is more secure than unencrypted traffic. Unencrypted traffic can be easily sniffed or even altered by malicious 3rd party.
WiFi AP	Use WPA2-PSK (AES) encryption	This is the most secure option. It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol
	Use WiFi AP strong key (password/passphrase)	"If malicious 3rd party is able to capture encrypted 4-way handshake, with strong password, decryption time can increase up to n years.
	Separate clients	Separate clients also known as wireless client isolation is a security feature that prevents wireless clients from communicating with one another. This feature adds additional level of security to limit attacks and threats between devices connected to the wireless networks.

WiFi Hotspot	Setting up a guest network for visitors	By setting up a guest Wi-Fi. A guest Wi-Fi network is essentially a separate access point on your router with separate IP pool. For example with guest network malware that somehow ended up on a guest's smartphone will not be able to get into your main business LAN
	Hotspot configuration	Setup data bandwidth limit. In that case malicious 3rd party will be unable to drain all your bandwidth. Use session time limit. In that case malicious 3rd party will be unable to drain your mobile data limit
WiFi SSID	Don't broadcast your router details	Service set identifier (SSID) should be changed. Default name will broadcast your device model.
DNS server	Don't use your Internet Service Providers (ISP) default Domain Name System (DNS)	There may come a time when the DNS servers used by your ISP come under attack, by a distributed denial-of-service (DDoS) attack, for example, or someone changing the DNS to effect a cloned banking fraud.
Password	Always use only strong passwords	Strong password requirements: • Has 12 characters, minimum; • Includes numbers, symbols, capital letters, and Lower-Case Letters; • Isn't a dictionary word or combination of dictionary words; • Doesn't rely on obvious substitutions. You can check your current password strength here: https://howsecureismypassword.net/"
Firmware update	Keep firmware up to date	With new firmware comes a lot of improvements: • Security fixes; • Performance enhancements; • Visual updates; So where is no reason why you shouldn't update firmware.
Secure firmware update	Always update firmware from official website	Always update firmware downloaded from our official page or use firmware over the air (FOTA).
RMS	Use RMS for remote access to the router	Disable remote access to your public IP and use RMS for remote management instead. You can find more details about RMS here: https://teltonika-networks.com/product/rms/
Unused features	Turn off router features you don't use that could pose a security risk	This would include remote access, Universal Plug and Play (UPnP), etc...
Common sense	Always use common sense while configuring any network device	-

RUT2xx security features

In the table below you can find all the security features supported by Teltonika's **RUT2xx** devices.

Security measurement type	Security measurement name	By default	Details
DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
	Remote ICMP Requests	On	An Internet Control Message Protocol (ICMP) flood attack, also known as a Ping flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
	SSH Attack Prevention	Off	A Secure Shell (SSH) flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with SSH requests.
	HTTP Attack Prevention	Off	A Hypertext Transfer Protocol (HTTP) flood attack is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with HTTP requests.
	HTTPS Attack Prevention	Off	Hypertext Transfer Protocol Secure (HTTPS) flood attack is same as HTTP flood attack but using HTTPS protocol instead of simple HTTP
Port Scan Prevention	Port Scan	Off	A port scan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port.
	SYN-FIN attack	Off	An attacker may send TCP/IP packets with the SYN and FIN TCP/IP flags set to a target system, ranging across all ports, to find open TCP/IP ports for further attacks. The target system will drop packets which are destined to open ports and send back RST/ACK packets for closed ports. The attacker may gather information from the system responses.
	SYN-RST attack	Off	SYN-RST attack, also known as TCP reset attack, is an abrupt closure of the session which causes the resources allocated to the connection to be immediately released and all other information about the connection is erased. TCP reset is identified by the RESET flag in the TCP header.
	X-Mas attack	Off	Christmas Tree (X-Mas) Attack is designed to send a very specifically crafted TCP packet to a device on the network. This crafting of the packet is one that turns on a bunch of flags. There is some space set up in the TCP header, called flags. And these flags all are turned on or turned off, depending on what the packet is doing.
	FIN scan	Off	FIN packets can bypass firewalls without modification. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP.
	NULLflags attack	Off	A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags. In a production environment, there will never be a TCP packet that doesn't contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and routers that filter incoming packets with particular flags.

Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Block Unwanted Access	SSH Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block SSH access from that source.
	WebUI Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block WebUI access from that source.
Configuration via SMS	SMS Utilities	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Plug and Play	UPnP	Not installed / Off	UPnP doesn't require any sort of authentication from the user. Any application running on your computer in LAN can ask the router to forward a port over UPnP, which is why the malware can abuse UPnP. Recommendation - If you don’t use it when leave it not installed or turned off.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

RUT850 security features

In the table below you can find all the security features supported by Teltonika's **RUT850** device.

Security measurement type	Security measurement name	By default	Details
DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
	Remote ICMP Requests	On	An Internet Control Message Protocol (ICMP) flood attack, also known as a Ping flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
	SSH Attack Prevention	Off	A Secure Shell (SSH) flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with SSH requests.
	HTTP Attack Prevention	Off	A Hypertext Transfer Protocol (HTTP) flood attack is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with HTTP requests.
	HTTPS Attack Prevention	Off	Hypertext Transfer Protocol Secure (HTTPS) flood attack is same as HTTP flood attack but using HTTPS protocol instead of simple HTTP

Port Scan Prevention	Port Scan	Off	A port scan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port.
	SYN-FIN attack	Off	An attacker may send TCP/IP packets with the SYN and FIN TCP/IP flags set to a target system, ranging across all ports, to find open TCP/IP ports for further attacks. The target system will drop packets which are destined to open ports and send back RST/ACK packets for closed ports. The attacker may gather information from the system responses.
	SYN-RST attack	Off	SYN-RST attack, also known as TCP reset attack, is an abrupt closure of the session which causes the resources allocated to the connection to be immediately released and all other information about the connection is erased. TCP reset is identified by the RESET flag in the TCP header.
	X-Mas attack	Off	Christmas Tree (X-Mas) Attack is designed to send a very specifically crafted TCP packet to a device on the network. This crafting of the packet is one that turns on a bunch of flags. There is some space set up in the TCP header, called flags. And these flags all are turned on or turned off, depending on what the packet is doing.
	FIN scan	Off	FIN packets can bypass firewalls without modification. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP.
	NULLflags attack	Off	A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags. In a production environment, there will never be a TCP packet that doesn't contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and routers that filter incoming packets with particular flags.
Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Block Unwanted Access	SSH Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block SSH access from that source.
	WebUI Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block WebUI access from that source.
Configuration via SMS	SMS Utilities	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

RUT9xx security features

In the table below you can find all the security features supported by Teltonika's **RUT9xx** devices.

Security measurement type	Security measurement name	By default	Details

DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
	Remote ICMP Requests	On	An Internet Control Message Protocol (ICMP) flood attack, also known as a Ping flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
	SSH Attack Prevention	Off	A Secure Shell (SSH) flood attack, is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with SSH requests.
	HTTP Attack Prevention	Off	A Hypertext Transfer Protocol (HTTP) flood attack is a common denial-of-service attack in which an attacker attempts to overwhelm a targeted device with HTTP requests.
	HTTPS Attack Prevention	Off	Hypertext Transfer Protocol Secure (HTTPS) flood attack is same as HTTP flood attack but using HTTPS protocol instead of simple HTTP
Port Scan Prevention	Port Scan	Off	A port scan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port.
	SYN-FIN attack	Off	An attacker may send TCP/IP packets with the SYN and FIN TCP/IP flags set to a target system, ranging across all ports, to find open TCP/IP ports for further attacks. The target system will drop packets which are destined to open ports and send back RST/ACK packets for closed ports. The attacker may gather information from the system responses.
	SYN-RST attack	Off	SYN-RST attack, also known as TCP reset attack, is an abrupt closure of the session which causes the resources allocated to the connection to be immediately released and all other information about the connection is erased. TCP reset is identified by the RESET flag in the TCP header.
	X-Mas attack	Off	Christmas Tree (X-Mas) Attack is designed to send a very specifically crafted TCP packet to a device on the network. This crafting of the packet is one that turns on a bunch of flags. There is some space set up in the TCP header, called flags. And these flags all are turned on or turned off, depending on what the packet is doing.
	FIN scan	Off	FIN packets can bypass firewalls without modification. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP.
	NULLflags attack	Off	A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags. In a production environment, there will never be a TCP packet that doesn’t contain a flag. Because the Null Scan does not contain any set flags, it can sometimes penetrate firewalls and routers that filter incoming packets with particular flags.
Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Block Unwanted Access	SSH Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block SSH access from that source.
	WebUI Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block WebUI access from that source.
Configuration via SMS	SMS Utilities	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Plug and Play	UPnP	Not installed / Off	UPnP doesn't require any sort of authentication from the user. Any application running on your computer in LAN can ask the router to forward a port over UPnP, which is why the malware can abuse UPnP. Recommendation - If you don’t use it when leave it not installed or turned off.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

RUTXxx security features

In the table below you can find all the security features supported by Teltonika's **RUTXxx** devices.

Security measurement type	Security measurement name	By default	Details
DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Block Unwanted Access	SSH Access Secure	On	By default, device allows a maximum of 5 login attempts (user defined). If all attempts are used, device will block SSH access from that source.
Configuration via SMS	SMS Utilities (Only in RUTX09 and RUTX11)	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Plug and Play	UPnP	Not installed / Off	UPnP doesn't require any sort of authentication from the user. Any application running on your computer in LAN can ask the router to forward a port over UPnP, which is why the malware can abuse UPnP. Recommendation - If you don’t use it when leave it not installed or turned off.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

TRB14x security features

In the table below you can find all the security features supported by Teltonika's **TRB14x** devices.

Security measurement type	Security measurement name	By default	Details
DDOS Prevention	SYN Flood Protection	On	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Access Control	Remote SSH access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTP access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote HTTPS access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Remote CLI access	Off	All Remote access is disabled by default. If user is using remote access feature it may be a security threat. If user decides to use this feature - it is recommended to use a strong password.
	Local SSH access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTP access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
	Local HTTPS access	Off	By default turned off - where is no scenario where HTTPS usage would be needed "out side the box".
	Local CLI access	On	Enabled by default for user convenience, allows possibility of configuring the device when user is in the same LAN.
Configuration via SMS	SMS Utilities	By router admin password	Default authorization method for configuration via SMS command is by router admin password. It's very important to have a strong password for admin account.
Default admin password	First login	On	Default password for Teltonika's devices is admin01 (weak password) but on first login to WebUI - RutOS forcefully requires user to change it. It is recommended to use a strong password
Certificates	Root CA	Pre-uplouded	Root CA certificate are only needed if you want to use HTTPS for your services. There is a default file already preloaded in this device which will be overwritten by any uploaded file.
Universal Asynchronous Receiver – Transmitter	UART	By router admin password	Many manufacturers are implementing UART interfaces on their devices. If this interface is not password protected, security of the device may be compromised. If malicious 3rd party gains physical access to the device it will have full control of the router via UART interface, this is a reason why our devices have password protected UART interfaces.

Active services

In the table below you can find all the services, which are enabled on default configuration in Teltonika's devices.

Service	Port	LAN	WAN
SSH	22	Open	Closed
HTTP	80	Open	Closed
HTTPS	443	Open	Closed