



Firmware for TN-4900 Series Release Notes

Version: v3.13	Build: 24100800
Release Date: Oct 09, 2024	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

- Added support for the Loopback Interface function.
- Added support for event-triggered actions to the VRRP function.
- Added support for UDP-Flood to the DoS Policy function.
- Added SNMP Trap as a Log Destination for the Layer 2 Policy function.
- Added support for additional event log export formats: .pdf, .csv.
- Added a CPU usage threshold alarm to the Event Notifications function.
- Added a port usage threshold alarm to the Event Notifications function.
- Added support for Step7 Comm+, OPC UA, and MELSEC to the Advanced Protection function.
- Added support for save and restore to the Custom Default function.
- Added support for the DNS Server function in Network Service.

Enhancements

- Enhanced the following IPsec algorithms:
 - Encryption: AES-256-GCM
 - Hash: SHA-512
 - DH Group: DH15 (modp3072), DH16 (modp4096), DH17 (modp6144), DH18 (modp8192), DH22 (modp1024s160), DH23 (modp2048s224), DH24 (modp2048s256), DH31 (curve25519)
 - PRF: PRF SHA-256, PRF SHA-384, PRF SHA-512
- Added a syslog option for VRRP State Change notifications.
- A detailed log message will now be recorded when importing a configuration fails.
- Supported Multiple Static Multicast Route Rules can be created with the same group address & outbound interface but different inbound interfaces.
- Added support for DHCP error logs in Event Notifications.
- Added support for IGMP Snooping error log in Event Notifications.
- Added support for the TRDP protocol to the Advanced Protection function in the CLI.
- Added support for RFC 5424 format for syslog messages.
- Added support for Default Action Log to the Layer3-L7 Policy function.

Bugs Fixed

- The "Login Authentication Failure Message" does not save properly.
- Using the newline character (\n) in the 'Login Message' and 'Login Authentication Failure Message' causes abnormalities in the output.
- The system is unable to ping the VRRP virtual IP.
- Users are able to bypass password policy violation warnings by pressing ESC on the keyboard.
- Time zone settings are not saved if GMT is set to 0.
- Port-based DHCP provides the same IP if those ports are member ports of a created bridge interface.
- RSTP is not functioning correctly over VLAN trunk ports.
- RSTP on VLAN trunk ports is causing a dual root device situation.
- Only one static multicast address can be configured at a time using the CLI or web import.



- SNMP OID returns an additional "\n" character.
- NAT is not working after reboot.
- op-up window will stay after auto logout.
- CVE-2024-6387 vulnerability issue. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-246387.
- CVE-2024-9137, CVE-2024-9139 vulnerability issues. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-241154.
- CVE-2024-1086 vulnerability issue. For more details, search the Security Advisories section on the Moxa website using the following Security Advisory ID: MPSA-249807.

Changes

- Changed the IPS license expiration behavior: When the license expires, IPS functionality will remain enabled, but IPS patterns will no longer be updated.
- Changed the Trusted Access behavior: Trusted Access now applies to the Web UI, CLI, and New Moxa Command interfaces.
- Changed the Preempt Delay range for the VRRP function from 10 to 300 to 0 to 300.
- Changed the maximum password and shared key length to 64 characters.
- The password and shared key now support special characters.

Notes

- If you encounter unexpected behavior with ECSP control packets, try disabling the Trusted Access Function first. If the issue persists, please contact the Moxa Technical Support team.



Version: v3.6	Build: 24032802
Release Date: Mar 29, 2024	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

- Adds the Fault LED to the hardware interface.

Enhancements

- Enhances and hardens the command injection method to increase security and prevent attacks.

Bugs Fixed

- A display error in the listing of available characters for the password policy.

Changes

- Changes the DoS Policy for Flood Protection to allow independent limit ranges for each interface.
- Changes ETBN functionality to enable status acquisition of master and backup via TRDP when using VRRP.

Notes

N/A



Version: v3.4	Build: N/A
Release Date: Jan 26, 2024	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

- Added support for TACACS+ authentication.
- Added Port Disable ingress action for Rate Limit function.
- Added support for LAN ID to DHCP Option 82 in the DHCP relay agent.
- Added support for Proxy ARP for LAN interfaces.
- Added support for Soft Lockdown mode to the Firewall function.

Enhancements

- Increased maximum number of static multicast entries from 256 to 1000.
- Increased the maximum username length to 32 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
- Increased the maximum length of passwords, communities, and shared keys to 64 characters for local account, SNMP, RADIUS, and IEEE 802.1X authentication.
- Unified the range of supported special characters for local account, SNMP, RADIUS, and IEEE 802.1X.

Bugs Fixed

- Network statistics values are inaccurate when using ports for measurement.
- The IP packets of IGMP do not contain a router alert.

Changes

N/A

Notes

N/A



Version: v3.0	Build: N/A
Release Date: Aug 30, 2023	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

- Added support for Network Security Package version 7.0 or higher (including TRDP protocol filter objects).
- Added the Auto Create Source NAT setting for 1-to-1 NAT.
- Added a Range option for the 1-to-1 NAT Destination IP Mapping Type.
- Added support for user-defined Engine ID to the SNMP function.
- Added support for SFTP to the Configuration Backup and Restore function.
- Added support for Firmware Version Checking to the Configuration Backup and Restore function.
- Added support for Password Max-life-time to the Password Policy function.
- Added support for NTP Authentication to the System Time function.
- Added support for Syslog Authentication to the Syslog function.
- Added support for Layer 2 Policy firewall logs to the Event Log function.
- Added support for DHCP Relay Agent to the DHCP server function.
- Added support for Intrusion Prevention System (IPS) functionality through Network Security Packages.
- Added Session Control Firewall Policy settings to the Firewall function.

Enhancements

- Compliance with the IEC 62443-4-2 industrial cybersecurity standard.
- Increased the maximum DHCP lease time from 99,999 to 527,039 minutes.
- Increased the maximum number of Zone-based Bridge interfaces from 2 to 4.
- Increased the maximum number of VLANs from 16 to 32.
- Increased the maximum number of Static Multicast Table entries from 128 to 256.
- Updated the web user interface to the latest next-generation design.
- Layer 3-7 firewall policies are now object-based for better rule management.
- Improved firewall log categories and information layout for better readability.

Bugs Fixed

- Enabling Bridge Mode may sometimes cause the system to perform a cold restart.
- Users are unable to change the VID of the Management VLAN.
- The SNMP encryption key incorrectly allows the use of illegal characters.
- When specifying a 64-character long IPsec pre-shared key, the system will incorrectly store it as 63 characters long.
- The SSH connection will randomly disconnect when using a non-default port configuration.
- Importing configurations will fail if Daylight Saving is enabled.
- The auto logout function of the login policy does not function properly.
- Enabling the Digital Input notification causes the STATE LED to turn red.
- Static routing does not function properly after enabling dynamic routing.
- The Turbo Ring becomes unstable after enabling the NTP/SNTP server.

Changes

- Changed the HTTP port range from 1-65535 to 1024-65535 (default port: 80).
- Changed the HTTPS port range from 1-65535 to 1024-65535 (default port: 443).
- Changed the Telnet port range from 1-65535 to 1024-65535 (default port: 23).



- Changed the SSH port range from 1-65535 to 1024-65535 (default port: 22).
- Changed the maximum length of the Bridge Zone name from 13 to 12 characters.

Notes

- Due to significant changes made in this firmware release, configuration files of previous firmware versions are not compatible with this version. Please create a new configuration using this firmware version. If you encounter issues when using this new firmware, please contact Moxa technical support.

Version: v1.2	Build: N/A
Release Date: Dec 28, 2022	

Applicable Products

TN-4900 Series

Supported Operating Systems

N/A

New Features

- Added support for PoE.
- Added support for DHCP Client Option 66/67/82.
- Added support for DHCP Relay Agent.
- Added support for Security Wizard (MXview).

Enhancements

- The CLI now supports digital signatures and data encryption.
- [IEC-61375-2-3] Local consist information now includes vehProp and cstProp.

Bugs Fixed

- [IEC-61375] If the device configuration contains IEC-61375 local-consist-info vehicle settings, importing the configuration will fail.
- [IEC-61375] NAT rules are not being applied correctly when using EBTN functions at the same time.
- [Rate Limiting] If the default Ingress Policy settings are changed, the Rate Limit function will behave abnormally and cause Rate Limit configuration importing to fail.
- [Firewall] Firewall Layer 2 policies do not work properly on zone bridge interface VLANs.
- [Event Log] When the topology is changed while using RSTP, the system does not record a topology change event log.
- [Turbo Ring v2] Incompatibility with some Moxa L2 switches.
- [Turbo Ring v2] Turbo Ring v2 becomes unstable when links are changed.
- [System File Update] The settings of VLAN 61375 change from Trunk to Access PVID 1 after importing the device configuration.
- [DHCP Server] The IP port binding entry cannot be set if the DNS Server 2 and NTP Server values have not been specified.
- [Bridge mode] Users are unable to set the IP of the bridge interface port.
- [MAC Address Table] The MAC address table filter function does not work when the device has trunk groups.
- [Certificate Management] The Local Certificate information shows incorrectly after importing a certificate.
- [RSTP] RSTP uses 50 to 60% of the CPU.
- [SNMP] After exporting the configuration file, the SNMP encryption type is incorrect.
- [Security] The 802.1X Server Key and PPTP password are not encrypted in the configuration file.
- [CLI] Some CLI descriptions are incorrect.
- [Web] The LAN (non-management VLAN) setting changes from Disable to Enable after exporting and importing the configuration back to the system again.
- [CLI] The NAT redundancy command is unable to set the VRRP binding index.
- [System File Update] Importing a configuration will fail when the web interface login message and login authentication failure messages are configured to the maximum character length.
- [Web] The number of system events recorded in the web and CLI interface is different.
- [Vulnerability] MPSA-221103
- [Vulnerability] MPSA-221105
- [Vulnerability] MPSA-221106
- [Vulnerability] MPSA-221201



Changes

- Removed unsupported functions from the web interface (Fiber, Relay).

Notes

N/A