Firmware for TN-4500B Series Release Notes

Version: v2.1	Build: 2026_0626_1733
Release Date: Jul 31, 2026	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• Support reserved port (internal loopback port) on RSPAN.

For details, please refer to the product web page and its user manual.

Enhancements

• MACsec Enhancement - Allow user to configure priority value in MKA PDUs for Key Server (KS) Election.
• MAC Authentication Bypass (MAB) Enhancement - MAB support MS-CHAPv2 and PAP.
• RSPAN - VLAN IDs are now listed in ascending order within the RSPAN dropdown list.

Bugs Fixed

• [CVE-2025-1680] Host Header Injection in Web Interface. For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: [MPSA-257421].
• The DHCP DNS settings field does not permit the use of the period (.) character.
• 802.1X local database authentication fails intermittently.

Changes

Not applicable.

Notes

Not applicable.

Version: v2.0	Build: 2025_0917_1811
Release Date: Dec 31, 2025	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• MAC Security (MACsec)
• mDNS Responder, support for ITxPT inventory
• DHCP Client Option 66/67 support for SFTP
• DHCP Server Option 66/67
• Auto Config - Debug Log
• Support for CEF/RFC-5424 syslog message format

For detailed specifications, please refer to the product page and user manual.

Enhancements

• IEC 62443-4-2 SL2 & ITxPT certified
• MAB/Dot1X enhancement - VLAN assignment
• Extended spec for ACL rules & QoS scheduler
• SSL certification operation process improvement
• MRP enhancement: Support for MRP interconnection mode
• Spanning Tree enhancement: Support for BPDU/Root/Loop Guard & BPDU filter
• NTP authentication type now supports AES-128.
• Added event log for "Event logs have been cleared."
• Support for PEAP for 802.1x with Local DB
• The “Admin” account cannot be deleted
• SPAN/RSPAN (mirror control packet)
• Enlarged DHCP Snooping entry limit from 32 to 256
• Added Trap/Email Event Notifications to Port Settings

Bugs Fixed

• For the last 4 ports in the 'Show interfaces status' CLI command, the negotiation field incorrectly shows 'No-negotiation'.
• When IGMP and LAG are enabled on the DUT, and IGMP membership reports are received from the trunk port, the group table does not record the port. The issue is a display discrepancy; IGMP Snooping and Port Trunking are functioning correctly.
• The mail server receiving event notification packets from the DUT may incorrectly display the IP as 127.0.0.1. The issue is a display discrepancy.
• TrapV1 packets contain an incorrect agent-addr of 127.0.0.1, which doesn't match the DUT IP. However, this value doesn't affect trap functionality.
• When logging in with RADIUS authentication, the NAS-IP-Address value is always set to 127.0.0.1. Despite the incorrect NAS-IP-Address in the packet, RADIUS functionality remains unaffected.
• When PoE per port is disabled/enabled at the same time as a PD power outage for multiple rounds, there's a 1/1000 chance (approx.) that all ports will lose power. It recovers after a reboot.
• [CVE-1999-0524] ICMP Timestamp Request Remote Date Disclosure. For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: [MPSA-257311].
• [CVE-2002-20001] Resource Exhaustion Vulnerability in Diffie-Hellman Key Exchange Protocol. For more details, search the Security Advisories section on the Moxa website for the following Security

Advisory ID: [MPSA-258261].

Changes

• Web UI/UX enhancement
• Support for new HW models: TN-4512B & TN-4516B PoE Full GE series. Please note that the TN-4512B & TN-4516B PoE Full GE series is only supported on firmware v2.0 and later. Users cannot downgrade to older versions such as v1.3, v1.2, v1.1, or v1.0 for Full GE series devices.
• Removed MAB clear web button

Notes

• The NTP authentication key string is displayed in plain text in the SNMP interface.
• The IGMPv3 group membership interval function works, but the current design only has a per-port timer, not a per-host timer. This leads to earlier timer expirations but has minimal impact on overall behavior. Multicast transmissions can be resumed by resending join requests as needed.
• The 'The bootfile name is invalid' syslog packet is not sent immediately, but after a few seconds.
• After creating a port trunk and then removing it, the QoS port priority does not return to the default. This is a complex interaction between LA and QoS functionalities that manifests under particular operational scenarios.
• The email function for sending 802.1x authentication failure logs is not working, while syslog and trap messages are being sent as expected.
• Under MSTP+GVRP topology, dynamic GVRP is abnormal and cannot learn VLANs correctly. MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to reconverge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability. Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.
• Reboot may occur during the import configuration process with a probability of around 1/10000.
• When executing the 'show' command via CLI, there is a low probability (<1%) of no output being displayed. Re-executing the command resolves this issue.
• A login failure may occur during the import configuration process with a probability of around 1/10000.
• A PD does not immediately power down upon reaching the scheduled time but experiences a brief delay of a few seconds.
• The syslog message "Insufficient information to propagate" generated by the Auto Configuration function is delayed by about a minute, but the timestamp within the frame is accurate.
• The IGMPv3 group table displays an incorrect status, but the packet behavior is as expected.
• Under TCMS Testbed with SPAN/RSPAN enabled, a cold start of a single DUT may occasionally encounter a login failure scenario where all ports remain in a down state. To recover from this, the device will have an automatic reboot, which may occasionally (2/10000) take up to 1 minute and 45

seconds to boot up.
• After configuring PoE, a cold start of a single DUT may occasionally encounter a login failure. To recover from this, the device will have an automatic reboot, which may occasionally (2/10000) take up to 9+ minutes to boot up.

Version: v1.3	Build: N/A
Release Date: Sep 03, 2025	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• Added support for TN-4524B. Please note that only firmware v1.3 and later support TN-4524B devices. Users cannot downgrade to older versions such as v1.2, v1.1, or v1.0 for TN-4524B devices.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

• Refer to notes for v1.1.

Version: v1.2	Build: 2025_0217_1155
Release Date: Mar 07, 2025	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• VLAN Unaware mode

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

Refer to notes for v1.1.

Version: v1.1	Build: N/A
Release Date: Feb 07, 2025	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• Turbo Ring V2 with Dynamic Ring Coupling (DRC)

Enhancements

• The Auto Configuration feature now implements Web UI Dependency.
• Prevent simultaneous enabling of ACL and LA.
• New Moxa command supports importing custom configurations with the admin password

Bugs Fixed

• Web DUT login lockout fails. Even after multiple incorrect password attempts, users can continue to try.
• After configuring Port Trunk, the port status displayed has errors when checking through CLI.
• The NAS-IP-Address for RADIUS authentication is always fixed at 127.0.0.1.
• The MAC address table does not update after configuring static multicast and adding a port to a VLAN.
• CLI DUT login lockout fails. Even after multiple incorrect password attempts, users can continue to try.
• Single DUT cold start has a 1/2500 chance of failing to log in. It recovers after a reboot.
• Under TCMS Testbed testing, a single DUT cold start has a 1/1500 chance of failing to log in with all ports link down.
• After enabling the 'File Signature' feature, the previously configured user-defined encryption key will reset to its default value. The user will need to reconfigure the encryption key in order to import configuration files encrypted by the user-defined key.
• After joining multiple L2 multicast groups using GMRP, the TN-4500B fails to populate its MAC table with new multicast group entries. Refreshing the table results in an error.

Changes

• Added TN-4524B Virtual Panel to Web Console: Supports new TN-4500B HW model (24 ports).
• MRP ring ports do not support Access switchport mode. Spec changed due to current chip limitation.

Notes

• NTP auth key string shown in plain text in SNMP interface.
• IGMPv3 group membership interval function works, but currently only has a per-port timer, not a per-host timer, leading to earlier timer expiration, but has minimal impact on overall behavior. Multicast transmissions can resume by resending join requests as needed.
• 'The bootfile name is invalid' syslog packet is sent after a few seconds and not immediately.
• After creating a port trunk and then removing it, QoS port priority doesn’t return to default due to complex interactions between LA and QoS under some scenarios.
• Last 4 ports in the 'Show interfaces status' CLI command incorrectly show 'No-negotiation' in the negotiation field.
• LACP doesn’t work after configuration on TN-4500A and TN-4500B Series due to LACP spec differences between TN-A and TN-B platforms.
  To mitigate this, on the TN-4500B, before configuring a port as a trunk member, set the port to 'Forced highest speed mode' then enable link aggregation to facilitate normal operation.

• When IGMP and LAG are enabled on DUT and trunk port receives IGMP membership reports, group table does not record the port. This is a display discrepancy; IGMP Snooping and Port Trunking are functioning correctly.
• Mail server receiving event notification packets from the DUT may incorrectly display the IP as 127.0.0.1. This is a display discrepancy.
• Email function for sending 802.1x auth failure logs is not working; syslog and trap messages are sent as expected.
• TrapV1 packets contain an incorrect agent-addr of 127.0.0.1, which doesn't match the DUT IP. This doesn't affect trap functionality.
• NAS-IP-Address value always 127.0.0.1 when logging in with RADIUS auth. This doesn't affect RADIUS functionality.
• If a static multicast is created before a VLAN member port is set, MAC address table is not updated.
The order in which settings are configured can lead to incorrect underlying value writes. This can be mitigated by configuring VLANs before creating static multicast groups or by rebooting.
• Under MSTP+GVRP topology, dynamic GVRP is abnormal and cannot learn VLANs correctly.
MSTP and GVRP are both VLAN-related. When VLAN changes dynamically, MSTP must reconverge, which can make the system unstable due to running complex operations. Using MSTP and GVRP together, this can result in network instability. It is recommended to avoid enabling both MSTP and GVRP.
• When PoE per port is disabled/enabled simultaneously with a PD power outage for multiple rounds, all ports may lose power (approx. 1/1000 chance). This recovers after a reboot.
• May reboot while importing a configuration (approx. 1/10000 chance).
• When executing the 'show' command via CLI, there is a low chance (<1%) of no output being displayed. Re-executing the command resolves this issue.
• Login failure may occur while importing a configuration (approx. 1/10000 chance).
• PD may have delay of a few seconds before powering down upon reaching the scheduled time instead of immediately powering down.
• Syslog message ‘Insufficient information to propagate’ generated by the Auto Configuration function delayed by about 1 min, but timestamp within frame is accurate.
• IGMPv3 group table shows incorrect status, but packet behavior is as expected.
• If RADIUS1 and RADIUS2 use different databases, after a failed Dot1x auth and exceeding the

quiet period, there is a chance the DUT will not send auth packets, resulting in auth failure. Manually triggering re-authentication can resolve the issue.
• Under TCMS Testbed with SPAN/RSPAN enabled, cold start of a single DUT may have a login failure issue where all ports remain down. To recover, the device will auto-reboot, which may (2/10000 chance) take up to 1 min 45 sec to boot.
• After configuring PoE, cold start of a single DUT may have a login failure. To recover, the device will auto-reboot, which may (2/10000 chance) take up to 9+ min to boot.

Version: v1.0	Build: N/A
Release Date: Sep 24, 2024	

Applicable Products

TN-4500B Series

Supported Operating Systems

N/A

New Features

• Initial release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

• Single DUT cold start has a 1/2500 chance of failing to log in. It recovers after a reboot.
• In TCMS Testbed testing, a single DUT cold start has a 1/1500 chance of failing to log in with all ports link down. It recovers after a reboot. The framework may access the network module before it fully initializes, which may lead to anomalies. This is difficult to reproduce in common applications (multiple devices cold starting simultaneously). In current tests with 4 DUTs powered on and off simultaneously, trigger probability is 1/9757. Though rare, its consequences are substantial. It will be addressed in an upcoming VR update.
• Web & CLI DUT login lockout fails. Even after multiple incorrect password attempts, users can continue to try.
• Enabling 'File Signature' resets configured user-defined encryption key to default. Users will need to reconfigure the encryption key to import config files encrypted by a user-defined key.
• SNMP TrapV1 packets have an incorrect agent-addr of 127.0.0.1, which doesn't match the DUT IP. This doesn't affect trap functionality.
• NTP authentication key string displayed in plain text in the SNMP interface.
• For the last 4 ports in the 'Show interfaces status' CLI command, the negotiation field incorrectly shows 'No-negotiation'.
• LACP doesn't work after configuration on TN-4500A and TN-4500B Series due to LACP spec differences between TN-A and TN-B platforms. Mitigation for TN-4500B: Ensure proper operation of static link aggregation and LACP before configuring the port as a trunk member, set the port to 'forced highest speed mode', then enable link aggregation. This will facilitate normal operation.
• When PoE per port is disabled/enabled simultaneously with PD power outages for multiple rounds, there's a 1/1000 (approx.) chance for all ports to lose power. It recovers after a reboot.
• For MSTP+GVRP topology, dynamic GVRP cannot learn VLANs correctly. MSTP and GVRP are both VLAN-related, and when a VLAN changes dynamically, MSTP needs to reconverge, which can cause instability due to complex operations. Using MSTP and GVRP together may cause network instability, so it is recommended to avoid enabling both of them.
• When creating a port trunk then removing it, QoS port priority doesn't return to default. This is a complex interaction between LA and QoS that occurs under particular scenarios.
• IGMPv3 group membership interval function works, but current design only has a per-port timer, not a per-host timer, leading to earlier timer expirations but has minimal impact on overall behavior. Multicast transmissions can resume by resending join requests as needed.
• When IGMP and LAG are enabled on the DUT and IGMP membership reports are received from the

trunk port, the group table does not record the port. This is a display discrepancy; IGMP Snooping and Port Trunking are functioning correctly.
• If a static multicast is created before a VLAN member port is set, the MAC address table is not updated. Setting configuration order can lead to incorrect underlying value writes. Mitigation: Configure VLANs before creating static multicast groups, or reboot the device.
• When sending special format PTR packets to the DUT, the DUT replies with abnormal format DNS response packets. The expected response is ignoring the packet, but it unexpectedly replies without providing the required answer. This does not significantly affect functionality.
• When logging in with RADIUS auth, the NAS-IP-Address value is always 127.0.0.1. Despite an incorrect NAS-IP-Address in the packet, RADIUS functionality is unaffected.
• 'The bootfile name is invalid' syslog packet is not sent immediately, but after a few seconds.
• The mail server receiving event notification packets from the DUT may display the IP as 127.0.0.1. This is a display discrepancy.
• Email function for sending 802.1x authentication failure logs not working, but syslog and trap messages are sent as expected.