# Connexium Firmware History

TCSESM and TCSESM-E Switches

***Note:*** *Our firmware are continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal :*
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

| Version # | Date of Publication | Internal reference | Description |
|---|---|---|---|
| **SV9.11** | **12/2020** | PEP0594886R | Update for 'California Law SB-327'. The law mandates that any new device "contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time." This forces users to change the unique password to something new as soon as it's switched on for the first time.<br>Password must contain at least 8 characters which include upper-case characters, lower-case characters, numerical digits and special characters for this product. |
| **SV9.04** | **05/2018** | | Cable Test (Copper only). This feature tests the cable attached to an interface for short or open circuit. During the test the traffic is interrupted on this port. This is available in a new Web Interface entry in "Diagnostics" > "Ports" > "TP cable diagnosis". |
| | | | Added an HTTPS server including HTTPS certificate management |
| | | | Added Secure Shell-1 and Secure Shell-2 (SSH1 + SSH2) option |
| | | | 802.1x security with Radius Authentication |
| | | | Radius Authentication for SNMPv3 (web) |
| | | | Allows restricted management access for Web, Telnet, SSH, SNMP services. This is available in a new Web interface entry in "Security" > "Restricted Management Access" with a limit of 16 entries. |
| | | | Adds an Auto Disable feature where a port can be disabled by the switch if of an error condition that is encountered on the port. Auto Disable offers a recovery option which automatically enables a disabled port after a configurable time. |
| | | | Adds a software implementation of Overload Detection to control incoming traffic to a port along with hardware metering. If the configured threshold is exceeded, then the configured action, Auto Disable or Auto Disable with recovery, will be applied. |
| | | | Adds MAC based port security to the Auto Disable feature. |
| | | | Adds Link Speed and Duplex Monitor to the Auto Disable feature. Link Speed and Duplex Monitor allows a user to specify what speed-duplex combinations are allowed for a specific interface. |
| | | | Allows deactivation of the 'Service Shell'. Reactivation of the Service Shell cannot be performed in the field and requires returning the hardware for service. |
| | | | Allows 'System Monitor 1' option to enable or disable. This is available in "Diagnostics" > "Selftest" |
| | | | Configurable Command Line Interface (CLI) Login banner |

| | | | |
|---|---|---|---|
| | | | Configurable SNMP v1/v2 community synchronization. When activating the "Synchronize password to v1/v2 community" function when the password is changed, the device synchronizes the corresponding community name. |
| **SV8.09** | **02/2016** | | Update firmware to fix Cyber security vulnerability - SNMP v3 Authentication bypass.<br>The implementation of SNMP v3 contains a vulnerability that may allow authentication bypass if specially crafted packets are used. |
| | | | Update C-Tick symbol on label |
| **SV8.04** | **06/2014** | | Java support update |
| | | | MRP Sub Ring Alarm Contact Capability<br>The sub ring manager now has the capability to indicate alarm conditions in the sub ring using the relay contact on the terminal block of the switch. Since the sub ring manager can handle more than 1 sub ring, the sub ring manger would indicate the alarm condition of all sub rings connected with one signal contact only. (Limited to Connexium Extended Managed Switches TCSESM-E) |
| | | | Switch Configuration Signature.<br>For customers that need to know if someone has changed the configuration of the Managed Switch. This is important for documentation and accountability reasons. Every time a configuration is saved, the switch will generate a random sequence of numbers and/or letters as signature of the configuration. This signature changes randomly every time the configuration is changed and does not change back to its previous value. The random generated part of the signature has to be saved with the configuration to assure it stays the same after a reboot. The Configuration Signature value is located in the Load/Save web page. |
| | | | LLDP-MED (Layer Link Discovery Protocol - Media Endpoint Device)<br>LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones, Voice / Media Gateways, switches, etc. LLDP-MED allows endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled. |
| | | | Configuration Re-Boot<br>Gives the user the capability to trigger a delayed reboot or reload. The delay has to be given in seconds. There can be only one delayed reboot/reload active at a time. If a delayed reset is applied twice the old one is overwritten. |
| | | | GMRP Discard Unknown Multicasts<br>Normally, if the multicast address of multicast data packet received by the switch is not registered on this switch, this packet will be broadcasted within this VLAN. Whereas after enabling the unknown multicast dropping feature, when receiving multicast data packet with unregistered multicast address, the switch will drop this packet. In this way, the bandwidth is saved, and the efficiency of the system is enhanced. |
| | | | SNMP Tunneling over HTTP<br>Computer networks use a tunneling protocol when one network protocol (the delivery protocol) encapsulates a different payload protocol. By using tunneling one can (for example) carry a payload over an incompatible delivery-network, or provide a secure path through an untrusted network. |
| | | | CLI (Command Line Interface) Banner<br>The switch can output a login banner when a user wants to login to the user interface (Web-based interface or CLI). This banner can display special information or warning messages for the user, before logging in CLI or WEB. |
| | | | Ingress (inbound traffic) or Egress (outbound traffic) can be selected separately for Port Mirroring. |

| | | | |
|---|---|---|---|
| | | | EtherNet/IP: Configurable TTL<br>Since EtherNet/IP Edition 1.3, the TCP/IP Interface Object was extended by a field to configure the TTL of EtherNet/IP multicast packets. The condition of the TTL field is that if either TTL Value or Mcast Config is implemented as settable, both must be implemented as settable. Because of this, the requirement must be extended to add to the TCP/IP interface object as settable (and storable) values.<br>Configure the TTL >1 to allow EtherNet/IP Multicasts sent over routers.<br>There is no Web page interface available. It is only configurable via EtherNet/IP. |
| **SV6.14** | **03/2014** | | Update firmware to fix web interface not starting issue when JAVA V7 Update 51 implemented |
| **SV6.13** | **03/2014** | | Update firmware to fix year 2036 issue |
| **SV6.09** | **09/2012** | | MRP gets unstable if RM gets a fragmented ping |
| | | | RSR: VLAN assignment for port3 does not fit when using VLAN0 transparent mode |
| | | | WEB Interface does not check valid characters in example sysname |
| | | | Display of HW version is not correct in CLI show sysinfo |
| | | | Own DUHM frame must not be forwarded |
| | | | Hashing mode is not configurable on Soho |
| | | | Schneider: Ethernet/IP EDS file generation on device TCSESM163F2CS0 fails |
| | | | DataHasChanged flag is activated after reboot if RRK is deleted |
| | | | MAC address may be assigned to wrong port on multi device switch |
| | | | Frame priority dependent overload flag on soho (if not RRC Standby switch) |
| | | | SNMP V3 data encryption setting (means disable unencrypted data) can't be saved |
| | | | Status of SFP Receive power is sometimes wrong |
| | | | No ports active after clearing config (Portsec <=> SNMP Deadlock, sporadic) |
| | | | Device displays RMON command which is not available in the command options. |
| | | | RSTP aging parameter in BPDU not correctly evaluated on BPDU reception (One less HOP) |
| | | | Device does not allow to configure spanning tree version as STP via SNMP mode. |
| | | | Web-Interface Spanning-Tree Port menu displays wrong values at Designated Ports |
| | | | SNMPv3 passwords cannot be changed after deleting SNMPv1/v2 communities |
| | | | Autosensing is not working properly |
| **SV6.00** | **08/2011** | | TCSESM-E only - Dual Ring with RSTP protocol - 50 ms recovery time |
| | | | TCSESM-E only - Quality of Service (QoS) configured on a per port basis |
| **SV5.00** | **03/2011** | | TCSESM only - Ability to support MRP and RSTP from a single switch |
| | | | TCSESM only – Improve RSTP recovery time (TCSESM Switches only)<br>Propagation: 15 ms. Detection: for Twisted Pair is 15 ms, Fiber Optic: 35m |

| | | | |
|---|---|---|---|
| | | | TCSESM-E only – Provides FastHiper Ring feature with a recovery time 25 ms max recovery time for ring or 50 switches |
| | | | TCSESM-E only – Dual ring using a single switch |
| | | | TCSESM-E only – Combination of MRP and RSTP on a single switch |
| | | | TCSESM-E only – Ability to support two different MRP rings from one switch |
| **SV4.10** | **NA** | | TCSESM only - Filtering _ Shared VLAN Learning |
| | | | TCSESM only - Management – SNMP v1 and SNMP v3 have similar password option |
| | | | TCSESM only - Device Status Indication |
| | | | TCSESM only - Disable Learning Mode |
| | | | TCSESM only - Transmission of oversize packets |
| | | | TCSESM only - HTTP Config File Transfer |
| | | | TCSESM only - EthernetIP Protocol |