# Aginode Switch Management
## with Firmware *V7.06O* and Manager *V7.06B* *or later*

Release Notes KD558E36

**CONTENTS**

# 1. Important Notice

- From Release V3.67 the Release Notes for the indicated firmware functions and/or bug fixes apply only to switches with Management Hardware version HW3 and HW5.
- New Switch Manager functions, which are independent of the firmware used, continue to apply to switches with Management Hardware versions HW0, HW1 or HW2. The expanded functionality is listed in the “Manager – Basic Features” category.
- Firmware and Manager versions containing two lower-case letters after the version number (e. g. V5.01ab) are pre-releases. These versions may not have the new functions indicated below integrated in their manuals.
- Firmware and Manager versions containing one upper-case letter after the version number (e. g. V5.02A) are bug fix versions and do not provide extended functionalities.

# 2. Releases Notes

**Legend:**

| | |
|---|---|
| ✓ | = Function is supported by the respective firmware version or Manager |
| | = The function is not supported or not applicable by the respective firmware family or switch manager (LANactive Manager) |
| **HW2** | = Function requires management hardware version HW2 or higher |
| **HW3** | = Function requires management hardware version HW3 or higher |
| **HW5** | = Function requires management hardware version HW5 or higher |

## 2.1.1. Release V7.06O

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **Manager – Basic Features:** | | | |
| [from V7.06A]<br>Framework upgraded to .NET 8 | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V7.06A]:<br>Error with missing UserName in SwitchLock Table while opening the Device-Editor was fixed. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V7.05bu]<br>In CLI the command “co:nfig {alarm1\|alarm2} c:lear” has been added to clear alarms M1/M2.<br>On Web interface buttons have been added to the “Port+Alarm State” webpage to clear alarms M1/M2. | ✓ | ✓ | |
| [from V7.05my]<br>Support for the following office switch types with management hardware version 5.50 and 5.51 has been implemented:<br>80 GigaSwitch V5 TP SFP-2VI<br>81 GigaSwitch 641 Desk SFP-VI<br>82 GigaSwitch 642 Desk SFP-2VI | ✓ | | |
| [from V7.05nq]<br>In CLI and on Web interface the alarm parameters “Alarm Source” and “Time since last alarm” for Alarm Outputs M1 and M2 have been added.<br>In CLI for command “show alarms” those parameters are additionally shown now.<br>On Web those parameters are shown in group “Alarm Output State” of the “Port+Alarm State” webpage. | ✓ | ✓ | |
| [from V7.05or]<br>A mechanism to forward VLANs and SPBM I-SIDs to connected switches in a daisy chain network has been added. For this purpose, Fabric Attach (FA) Assignment TLVs are used to exchange VLANs and/or SPBM I-SIDs between the switches via LLDP. To control, whether VLAN and/or SPBM I-SIDs shall be sent via LLDP, or be learnt and added to the VLAN Table if received via LLDP, a VLAN Table Sending Mode and a VLAN Table Learning Mode have been introduced.<br>**Manager – Extensions:**<br>In the Device Editor, on tab “VLAN > VLAN Table”, two dropdown lists “VLAN Table Sending Mode” and “VLAN Table Learning Mode” have been added. | ✓ | ✓ | ✓ |
| [from V7.05re]<br>A Network Time Protocol (NTP) Client has been added as new Time Client. NTP allows clock synchronization with up to five time servers and an accuracy of less than one millisecond. To avoid Distributed Denial-of-Service (DdoS) attacks during NTP communication, NTP authentication using symmetric keys has been introduced as well.<br>**Manager – Extensions:**<br>In the Device Editor, on tab “Time Client”, a new tab “NTP Setup” to configure NTP parameters, time servers and authentication keys has been added. | ✓ | ✓ | ✓ |
| [from V7.05pm]<br>For Configuration Changed alarms the corresponding CLI commands for the changed configuration parameters have been added. | ✓ | ✓ | ✓ |
| [from V7.05sr]<br>Only applies to iGigaSwitches and XGigaSwitches with management hardware HW5 and PoE+ functionality for the 4 to 12 copper ports at the front panel:<br>Support for PoE+ adapter Rev.B has been implemented. | ✓<br>**XGiga Switch** | ✓ | |
| [from V7.05td]<br>The newly introduced mechanism to forward VLANs and SPBM I-SIDs to connected switches in a daisy chain network has been extended for VLAN-Names. For this purpose, Aginode has introduced a new Fabric Attach (FA) VLAN-Name TLV, to transfer the VLAN-Names of the VLANs and SPBM I-SIDs previously advertised by FA Assignment TLVs. To control, whether VLAN, SPBM I-SIDs and/or VLAN-Names shall be sent via LLDP, or be learnt and added to the VLAN Table if received via LLDP, the VLAN Table Sending Mode and VLAN Table Learning Mode have been extended by two more options.<br>**Manager – Extensions:**<br>In the Device Editor, on tab “VLAN > VLAN Table”, two options “Send VLANs and VLAN-Names” and “Send VLANs, SPBM I-SIDs and VLAN-Names” have been added to dropdown list “VLAN Table Sending Mode”, and two options “Learn VLANs and VLAN-Names” and “ Learn VLANs, SPBM I-SIDs and VLAN-Names” to dropdown list “VLAN Table Learning Mode”, respectively. | ✓ | ✓ | ✓ |
| [from V7.05ts]<br>Fabric Attach has been extended so that Aginode switches can learn and send Management VLANs to connected switches. For this purpose, the Management VLAN contained in Fabric Attach (FA) Element TLVs is read. | ✓ | ✓ | |
| [from V7.05uu]<br>Support for the following office switch types with management hardware version 5.50 and 5.51 has been implemented:<br>83 GigaSwitch V5 TP SFP-VI<br>99 XGigaSwitch V6 2SFP | ✓ | | |
| [from V7.06M]<br>Applies only to switches supporting HSR/PRP:<br>Forwarding of HSRP (Hot Standby Routing Protocol) packets over HSR/PRP has been implemented.<br>**Manager – Extensions:**<br>In the Device Editor, on tab “Redundancy > HSR/PRP”, a checkbox “HSRP (Hot Standby Routing Protocol) forwarding enable” has been added. | | ✓ | ✓ |

| | | | |
|---|---|---|---|
| [from V7.06N]<br>Static Link Aggregation after Power Up set wrong Port Forwarding State | ✓ | ✓ | ✓ |
| | | | |
| **Firmware – Security:** | | | |
| [from V7.05ng]<br>The HTTPS server certificate (RSA, 3072 Bit Key, SHA-256) has been extended with the SAN (Subject Alternative Name) "DNS=*.switch.Aginode". Furthermore a new CA certificate is required, which can be downloaded from the Aginode support page. Without this SAN extension, many current browser versions doesn't accept the server certificate and report a warning, even the corresponding CA certificate has been imported into the browser. See manual for a detailed description. | ✓ | ✓ | |
| [from V7.05nz]<br>A new authentication mode "TACACS+ first, then Local Accounts on timeout or reject" has been added for SCP, SSH, Telnet and V.24. In this mode, the TACACS+ authentication is done first. If the TACACS+ server is not reachable or the request is rejected, authentication by local accounts is performed.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Management > Access Global", option "TACACS+ first, then Local Accounts on timeout or reject" has been added to the Telnet, SSHv2, SCP and V.24 Authentication Modes.<br>Moreover, option "TACACS+ first, then local" has been renamed to "TACACS+ first, then Local Accounts on timeout only". | ✓ | ✓ | ✓ |
| [from V7.05nv]<br>For HTTPS access the factory default minimum protocol version has been set to TLS1.2. | ✓ | ✓ | |
| [from V7.05rp]<br>Support for customer HTTPS certificates has been added. With this feature the user can copy a customer-specific HTTPS certificate for HTTPS web sessions to the switch.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Management > Access Global", WEB Setup option "HTTPS Certificate" and a button to copy the customer-specific HTTPS certificate have been added. | ✓ | ✓ | ✓ |
| [from V7.05um]<br>The User account has been extended with a new configuration setting called "User Access rights". The available options are:<br>- Read/Only for all parameters<br>- Read/Only for all parameters except Delete Local Log (factory default)<br>**Manager – Extensions:**<br>In the Device Editor on tab "Management > Local Accounts" in group "User Account Setup (Read/Only)" the parameter "User Access Rights" has been added. | ✓ | ✓ | ✓ |
| [from V7.05wk]<br>If a RADIUS CoA or PoD request with unsupported attributes was received, the response was a CoA-NAK or PoD NACK error (Unsupported-Attribute). Now unsupported attributes are ignored. | ✓ | ✓ | |
| **Firmware – SNMP:** | | | |
| | | | |
| **Firmware – Redundancy:** | | | |
| | | | |
| **Firmware – Bug Fixes:** | | | |
| [from V7.05kh]<br>In CLI console for show commands with pagewise printing sometimes the output was cut off or interrupted by echoed key inputs. | ✓ | ✓ | |
| [from V7.05kh]<br>If TACACS+ Command Authorization was enabled, entered CLI commands were not always correctly authorized by the firmware according to the TACACS+ server configuration. | ✓ | ✓ | |
| [from V7.05ks]<br>The PoE power value in mW printed in PoE Overload Failure Alarm syslog messages was wrong. | ✓ | ✓ | |
| [from V7.05kx]<br>The Backup Firmware Version shown in Device Info was sometimes wrong when the switch was started with an SD card from another switch type. | ✓ | ✓ | |
| [from V7.05ms]<br>If the PoE input voltage was interrupted or out of lower/upper alarm limit, PoE was disabled on all PoE ports. Even if the PoE voltage was back, PoE remained disabled. | ✓ | ✓ | |
| [from V7.05mw]<br>If one device connected to the switch (e.g. an IP-phone) was authenticated via IEEE802.1X, and another device connected to the first device was authenticated via RADIUS, the IEEE802.1X learned MAC addresses could disappear from the MAC table after a random time. | ✓ | ✓ | |
| [from V7.05nh]<br>Every time a Renew or Save Configuration was performed and the user was logged into the Web interface, the user got disconnected because of a Web server restart and had to login again. Now the Web server is only restarted if the DHCP / IP parameters, or the Management VLAN have changed. | ✓ | ✓ | |
| [from V7.05nq]<br>If Flow Control mode was set to "Auto" and the user was logged into the Web interface, the user got disconnected after a short time again. | ✓ | ✓ | |
| [from V7.05nr]<br>Under very rare certain circumstances the switch stops sending RADIUS request in case of an IEEE802.1X re-authentication. | ✓ | ✓ | |
| [from V7.05oa]<br>Enabling IGMP snooping may result in IGMP multicast traffic being forwarded to the CPU management interface. Depending on the volume of multicast data traffic, this could affect management access. | ✓ | ✓ | |
| [from V7.05rf]<br>An Internal Warning code 109 was shown in Local Log under certain circumstances when the user tried to login to the Web interface multiple times. | ✓ | ✓ | |
| [from V7.05sp]<br>Only applies to XGigaSwitches with management hardware HW5 and PoE+ functionality for the 4 to 8 copper ports at the front panel:<br>The port mapping between the port a PoE device was connected and powered PoE port shown on the PoE State page was partially wrong. | ✓<br>**XGiga Switch** | ✓ | |

| | | | |
|---|---|---|---|
| [from V7.05wb]<br>Only applies to switches with firmware version V7.05rf or higher:<br>When the SNTP client was enabled and the switch rebooted, the switch was no longer accessible via the LANactive Manager but was still accessible via the CLI console or WEB interface. In addition, the correct time was not adopted during time synchronization. | ✓ | | |
| [from V7.05wk]<br>When the port for RADIUS CoA was changed, RADIUS CoA had to be manually turned off and on again to activate the port. | ✓ | ✓ | |
| [from V7.06C]<br>If DHCP was enabled and a longer lease time, e.g. 365 days, was configured, under some circumstances the switch went offline after about 33 days and was only reachable via LLDP. Only a DHCP renew caused the switch to get online again. | ✓ | ✓ | |
| [from V7.06F]<br>Only applies to GigaSwitches V5 with management hardware version 5.5x:<br>When the SNTP Client was enabled and the switch restarted after cold start or voltage interruption, the switch was not accessible anymore via Management interface, but still via CLI console or WEB interface. | ✓ | | |
| [from V7.06F]<br>Only applies to GigaSwitches V5 with management hardware version 5.5x:<br>The system uptime was running 60 minutes too fast per day. If SNTP/NTP time synchronization was enabled, the system time also runs too fast during the server request intervals. | ✓ | | |
| [from V7.06G]<br>Only applies to GigaSwitches V5 with management hardware version 5.5x:and six ports (switch type 83):<br>The function input was not working and therefore not shown at the management interfaces. | ✓ | | |
| [from V7.06I]<br>Only applies to V5 switches with management hardware versions 5.1x to 5.4x:<br>The Portmonitor did not work correctly for own packets sent by the switch on the Portmonitor source port.<br>Tx (egress) packets from the Portmonitor source port were not forwarded to the Portmonitor destination port. | ✓ | ✓ | |
| [from V7.06J]<br>Only applies to iGigaSwitches V5 hardware versions 5.x:<br>The MAC addresses learned on a port were not displayed under “MAC+Security state” in the Manager and under "show security" in the CLI. However, the MAC addresses were visible in the MAC Table. | | ✓ | |
| [from V7.06J]<br>For CLI command "show security" the same learned or fixed MAC address was shown up to 30 times for a port under certain circumstances. | ✓ | ✓ | |
| [from V7.06J]<br>Only applies to GigaSwitches V5 hardware versions 5.x and Rev. A PoE adapter:<br>The PoE input voltage was always indicated as 54 V, independent from the applied voltage. GigaSwitches can be powered with 54 V or 48 V power supplies. | ✓ | | |
| [from V7.06J]<br>Port Security was switched off by a firmware update, if the firmware was first downgraded from a version V7.0x to a version 6.0x or lower, and then upgraded again with Port Security settings to a version V7.0x.<br>Moreover, the Port Security settings were not adopted if a Master-Configuration created with version V6.0x or lower was copied to the switch with version V7.0x. | ✓ | ✓ | |
| [from V7.06J]<br>If a Master-Configuration with both DHCP and static IP settings configured and enabled was copied to the switch, the dynamically received DHCP-values were overwritten by the static IP settings. | ✓ | ✓ | |
| [from V7.06K]<br>If a PoE device was connected to the switch and the device requested first a lower power and then a higher power via LLDP on startup (e.g. a Cisco Phone with additional box), then the switch not always provided enough power to supply the device. | ✓ | ✓ | |
| [from V7.06K]<br>Only applies to switches with firmware version V7.01aa or higher:<br>If the speed mode of a Nexans Copper SFP was set to 10 or 100Mbit, data flow was blocked, even the link LED shows a link-up. | ✓ | ✓ | |
| [from V7.06O]<br>Only applies to V5 Office Switches with memory card (MC) inserted:<br>If the Config was written by LANactive Manager or CLI command, the switch slowed down and temporary went offline. | ✓ | | |

## 2.2. Release V7.04

### 2.2.1. Release V7.04L

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **Manager – Basic Features:** | | | |
| [from V7.04E]<br>Client/Controller: Implemented automatic referral chasing during Active Directory Authentication. | | | ✓ |
| [from V7.04E]<br>Client/Controller: csv files used in Master-Configs can now be uploaded from within the Managers File Management. Inside the Master-Config, csv files can also be uploaded and selected via a combobox. | | | ✓ |
| [from V7.04E]<br>From now on multiple firmware files can be selected to update different types of switches simultaneously. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Enhanced Active Directory Authentication to use any kind of LDAP Server. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V7.04E]<br>Client/Controller: Added setting to choose whether “Device blocked” message should be a warning which can be ignored or a blocking error. | | | ✓ |
| [from V7.04E]<br>Port VLAN Config has been added to the Inventory-List. | | | ✓ |
| [from V7.04E]<br>Setting “Preferences → Global → Sleep between retries” has been added. This parameter defines the time to wait before restarting any writing action (Config, Firmware Update…) after the previous one has failed. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Speed of importing Device-Lists has been greatly improved. | | | ✓ |
| [from V7.04E]<br>Client/Controller: By using a Role Template, users can be assigned to a specific port type like User Port instead of only a port number. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V7.04E]<br>While reading csv files from within a master config, the values are now checked for invalid characters. | | | ✓ |
| [from V7.04E]<br>Device-Editor → VLAN Table → Changing SPBM I-SID caused error message, that ID already exist even when ID is unique. | | | ✓ |
| [from V7.04E]<br>Client/Controller: The controller was not able to read date format “dd/MM/yyyy HH:mm:ss”. This has been fixed. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Referral chasing while authenticating against Active Directory did not work properly. | | | ✓ |
| [from V7.04E]<br>Firmware Update of family F50 showed error message “FAILED: Wrong firmware”. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Updating firmware by device time client did not work. The update started right away instead of waiting for the given date and time. | | | ✓ |
| [from V7.04E]<br>Client/Controller: When using “RADIUS first, then local” as authentication mode, local accounts where not used when RADIUS server are not available. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Old Switches in the database (firmware V3.xx) could cause the Device-List to fail loading after login. | | | ✓ |
| [from V7.04E]<br>Client/Controller: Reading connected devices via first TP port with the Basic-Configurator was not working. | | | ✓ |
| [from V7.04E]<br>SNMP Engine ID was not focused after validation failed. | | | ✓ |
| [from V7.04E]<br>Client/Controller: When using Integrated Security for Database Authentication, this value was reset automatically by the controller. | | | ✓ |
| [from V7.04E]<br>State of third RADIUS server could not be read from the Device-Editor, causing the Editor to crash. | | | ✓ |
| [from V7.04E]<br>Sometimes the Controller Service could not be stopped properly. This issue has been fixed. | | | ✓ |
| [from V7.04E]<br>Inventory List with MAC and LLDP information did not show Information of all ports. | | | ✓ |
| [from V7.04E]<br>“Device is offline” Label was not showing up inside the Device-Editor when switch went offline. | | | ✓ |
| [from V7.04E]<br>Basic Configuration was disabled on server side Layer 2 Autodiscovery. | | | ✓ |
| [from V7.04F]<br>Basic Configuration did not work properly while running the Controller on Linux. | | | ✓ |
| [from V7.04G]<br>Inventory-List: Changed manufacturing date format to ISO8601 (‘yyyy-MM-dd’). | | | ✓ |
| [from V7.04H]<br>Client/Controller: Firmware Update could not be started from within the Device-Editor. | | | ✓ |
| [from V7.04H]<br>Client/Controller: Under certain circumstances the server settings could not be loaded after login. | | | ✓ |
| [from V7.04H]<br>Device-Editor → Input/Output State: Wrong spelling of “Active” corrected. “Activ” → “Active” | | | ✓ |
| [from V7.04H]<br>Inside Log-Messages Time-Stamp day and month were swapped. | | | ✓ |
| [from V7.04I]<br>Using Active Directory or RADIUS Authentication could lead to loss of Client User Id and forever blocked switches. | | | ✓ |
| [from V7.04J]<br>Reading/writing Config did not work when using ‘IPv6 first, then IPv4’ and the Device was not reachable via IPv6. | | | ✓ |
| [from V7.04K]<br>Updating device to firmware V7.06A leads to an error message even though the update was successful | | | ✓ |
| [from V7.04L]<br>Client/Controller: Fixed IP Address was overwritten by configured IP Address in Device-List. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V7.03ap]<br>The output format of CLI command "show log" to show the Local Syslog has been improved so that content can be viewed pagewise with the space key. | ✓ | ✓ | ✓ |
| [from V7.04E]<br>Added parameter ‘no-pause’ to CLI command ‘sh:ow ma:c-address-table d:ynamic [{<if-no>\|a:ll}] [n:o-pause]’ to show whole MAC Address Table without pressing <space> key. | ✓ | ✓ | |
| **Firmware – Security:** | | | |
| | | | |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **Firmware – SNMP:** | | | |
| | | | |
| **Firmware – Redundancy:** | | | |
| [from V7.04B]<br>Compatibility of the MRP protocol with different third party vendors has been improved. | | ✓ | |
| [from V7.03ap]<br>Running MSTP (Multiple Spanning Tree Protocol) over a LAG (Link Aggregation Group) has been implemented.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Redundancy >Link Aggregation" the setting “MSTP Virtual Port” has been added | ✓ | ✓ | ✓ |
| **Firmware – Bug Fixes:** | | | |
| [from V7.03ak]<br>Problems while applying customer pre-configuration in factory have been resolved. | ✓ | ✓ | |
| [from V7.03af]<br>If MAC Flapping is set to “Don’t disable port. Send alarms only”, flapping MAC addresses are learned for all Security Modes with MAC address learning except "Learn & Fix". Hence, those MAC addresses are also visible in the “MAC+Security State” and in the Port Security MAC Address Table of the port. | ✓ | ✓ | |
| [from V7.03ap]<br>Only applies to switches with management hardware HW5:<br>The Spanning Tree topology calculation was wrong if using the MSTP protocol and if three or more switches are arranged in a ring. | ✓ | ✓ | |
| [from V7.03ap]<br>The output format of CLI command "show log" to show the Local Syslog has been improved so that content can be viewed pagewise with the space key. | ✓ | ✓ | |
| [from V7.03aq]<br>The cryptographic method TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 has been added to TLS1.2 | ✓ | ✓ | |
| [from V7.02ba]<br>Only applies to switches with management hardware HW5 and SD card inserted:<br>If the configuration was saved repeatedly within a short time, e.g. by entering multiple set commands in the CLI console, the switch hanged or slowed down for 20 to 30 seconds. This effect was distinct especially for HW5 7-Port Office GigaSwitches. | ✓ | ✓ | |
| [from V7.04B]<br>The PoE port mapping for iGigaSwitch 1002 with 4-port PoE+ adapter was not correct | | ✓ | |
| [from V7.04E]<br>Only applies to switches with management hardware HW5 and a copper uplink port with PoE-PD capability:<br>The PoE LED of port 5 wrongly lights red. Because this port has only PoE-PD capability, the port is not able to deliver PoE power and thus the corresponding PoE LED must be off. | ✓ | | |
| [from V7.04E]<br>Only applies to switches with management hardware with HSR/PRP support:<br>The CLI configuration of HSR/PRP protocol was wrong printed. | | ✓ | |
| [from V7.04E]<br>DHCP Snooping didn’t disable the port if the DHCP server sends Offer or Acknowledge packets with a UDP destination port number other than 68. | ✓ | ✓ | |
| [from V7.04F]<br>Only applies to Aginode switches cascaded over a fiber or copper port and had the spanning tree protocol enabled:<br>If a Cisco PVST+ packet with destination address 01:00:0c:cc:cc:cd was received within the Mgmt VLAN, this may result in a packet storm with this PVST+ packet under certain circumstances. | ✓ | ✓ | |
| [from V7.04G]<br>Enabling IGMP snooping may result in IGMP multicast traffic being forwarded to the CPU management interface. Depending on the volume of multicast data traffic, this could affect management access. | ✓ | ✓ | |
| [from V7.04G]<br>If one device connected to the switch (e.g. an IP-phone) was authenticated via IEEE802.1X, and another device connected to the first device was authenticated via RADIUS, the IEEE802.1X learned MAC addresses could disappear from the MAC table after a random time. | ✓ | ✓ | |

## 2.3. Release V7.02

## 2.3.1. Release V7.02F

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| **Firmware family HW3➔** | **HW3-Fxx-Pxx-OFFICE** | **HW3-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **Manager – Basic Features:** | | | |

| | | | |
|---|---|---|---|
| [from V7.02F]<br>Every communication with devices has been completely moved from client to controller. The client will now send a message to the controller to for example read the configuration or update the firmware instead of doing this itself. Also, the file system has been moved to the controller, but it is still possible to download local copies to the client. | | | ✓ |
| [from V7.02F]<br>PSCP.exe and Putty.exe have been updated to Version 0.74. | | | ✓ |
| [from V7. 02C]<br>A web interface has been added to the controller. This web interface offers every basic functionality needed to configure, update and observe any device without having any client software installed. | | | ✓ |
| [from V7.02F]<br>Checking of registration key and saving the registration data has been moved to the controller. That means, that only one client needs to register the product and the full functionality will be unlocked on all other clients. | | | ✓ |
| [from V7.02F]<br>A test button has been added to Server Settings → E-Mail Settings to check the connection to the SMTP server. | | | ✓ |
| [from V7.02F]<br>Client/Controller version now supports communication with transport layer security (https). | | | ✓ |
| [from V7.02F]<br>Client/Controller: SQL Express has been updated to SQL Express 2019. | | | ✓ |
| [from V7.02F]<br>Client/Controller: A pager has been added to the log message window | | | ✓ |
| [from V7.02F]<br>Client/Controller: New feature to import Predefined Devices from Database View has been added. This allows the user to select Devices inside the Database View and move them to the Predefined Device list with their current CLI configuration. Using the context menu in the main grid one MAC Address can easily be exchanged if any Device needs to be replaced. | | | ✓ |
| [from V7.02F]<br>Client/Controller: The "predefined" directory has been removed from the controller. Instead, the "configs" directory is used for any CLI Config file that is supposed to be used for mass configuration. Also script files are no longer stored in the "database" directory. The newly created "scripts" directory is used instead. | | | ✓ |
| [from V7.02F]<br>Client/Controller: RADIUS and Active Directory can now be used to authenticate and manage users and user rights. | | | ✓ |
| [from V7.02F]<br>.NET Framework has been upgraded to .NET 5. This includes that the Controller is now able to run on any operating system, for example LINUX. | | | ✓ |
| [from V7.02F]<br>Button "Move selected Devices to Device-List" has been added to Layer 2 Autodiscovery | | | ✓ |
| [from V7.02F]<br>Maximum number of simultaneously opened Device-Editors is not restricted to four anymore. This value can be configured using 'Preferences' → 'Device-Editor'. | | | ✓ |
| [from V7.02F]<br>Obsolete sections Device-Editor → Redundancy → Zeroloss and Device-Editor → DHCP Relay Agent have been disabled. | | | ✓ |
| [from V7.02F]<br>Device-Editor → Alarms → SFP Alarms: Button 'Set Limits for all Ports' has been added to set the limits for all ports at the same time. Also button 'Read Limits from Device' has been added to read all limits from the allowed range of the SFP information. | | | ✓ |
| [from V7.02F]<br>Device-Editor → VLAN → VLAN Table: It is now possible to enter multiple VLAN IDs to add or delete multiple VLANs at once. | | | ✓ |
| [from V7.02F]<br>Excel-like filtering mode has been added to the Device-List. This can be activated by setting Preferences → Device-List → Enable Excel-like filtering. | | | ✓ |
| [from V7.02F]<br>New settings "Show all subcategory devices" has been added to Preferences → Device-List. By enabling this setting, after selecting any category all devices in this category and all subcategories are shown. By disabling, only the Devices in this category are shown. | | | ✓ |
| [from V7.02F]<br>Client/Controller: Performance of the Poll Engine has been highly increased, which leads to very less CPU usage of the Controller. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V7.02F]<br>On tabpage 'Input/Output State' in the Device-Editor the Alarm Source displayed the name of a wrong device name. | | | ✓ |
| [from V7.02F]<br>If any maximum length of a textbox in the device editor is exceeded, a message box is shown. | | | ✓ |
| [from V7.02F]<br>A memory leak in the controller service has been fixed, which occurred when any client was logged in over a long time. | | | ✓ |
| [from V7.02F]<br>Client/Controller: An error message occurred when multiple instances of the LANactive Manager Client where started | | | ✓ |
| [from V7.02F]<br>Client/Controller: When the Controller was installed on a virtual machine, it was not able to start anymore after the VM has been moved or changed. This problem has been fixed. | | | ✓ |
| [from V7.02F]<br>Client/Controller: While starting multiple instances of the Web Interface, the username of the first user was automatically filled into the login screens of the other instances. | | | ✓ |
| [from V7.02F]<br>Client/Controller: Switches in a Category with a depth of 3 or more were not shown in the Device-List. | | | ✓ |
| [from V7.02F]<br>Client/Controller: Long processing times for server requests could freeze the Layer 2 Discovery dialog. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V7.02F]<br>Client/Controller: Overtaking another client users session did not work properly. | | | ✓ |
| [from V7.02F]<br>Client/Controller: On Device-Editor Tabpage Input/Output State the Alarm Source M2 was marked red with empty IP Address inside although no alarm was active. | | | ✓ |
| [from V7.02F]<br>Device-Editor → Management → Access SNMP → SNMPv3 Flexible Account Setup → Authentication Password could not be set using the Manager. | | | ✓ |
| [from V7.02F]<br>Client/Controller: Using https could cause random “Server Connection lost” error messages. | | | ✓ |
| [from V7.02F]<br>Device-Editor →Access List Ranges dialogs were too small to fit all content. | | | ✓ |
| [from V7.02F]<br>Client/Controller: While importing old Device-List files, Devices were not assigned to their corresponding categories. | | | ✓ |
| [from V7.02F]<br>Checking/Unchecking all parameters in Master-Config for DICE Switch caused an error message. | | | ✓ |
| [from V7.02F]<br>Client/Controller: When server connection is lost, Device-Editor did not stop polling, causing a lot of error messages written on the controller. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V7.01aa]<br>Only applies to iSwitches with PoE++ Adapter Type IEEE802.3bt:<br>Support for switches with PoE++ adapters according to IEEE802.3bt has been added. Those PoE++ adapters can provide up to 90 Watts for powering PoE devices (PDs) with power classes 5 to 8.<br>**Manager – Extensions:**<br>In the Device Editor a new PoE Setup mode “IEEE802.3bt” has been added. Furthermore, the existing PoE Setup modes have been renamed:<br>- “Auto 802.3af” to “IEEE802.3af / 15 W”<br>- “Auto 802.3af High-Power (Ignores Power Class)” to “IEEE802.3af / 30 W (Ignores Power Class)”<br>- “Auto 802.3at High-Power” to “IEEE802.3af / 30 W”<br>This applies for the following tabs:<br>- tab “Port Setup > Port <1...n>”, dropdown list “PoE Setup”<br>- tab “Global + Link State”, column “Power Setup”<br>- tab “PoE State”, column “Power Setup”<br>Moreover, on – tab “PoE State”, the last column has been renamed to “Power Class / Max. Power / Pairs” and now also indicates the number of pairs used for powering the PDs. | | ✓<br>**HW5** | ✓ |
| [from V7.01ch]<br>Only applies to certain switch types:<br>When replacing one switch type by another, e.g. in case of migration to a different hardware of the same firmware family, the switch configuration stored on the memory card will be automatically converted for the most frequent use cases. This feature is called Automatic Configuration Transfer (AutoConfigTransfer). | ✓ | ✓ | |
| [from V7.01fk]<br>The maximum value of “PoE Input Power Limit” has been increased to 1000W for PoE++ IEEE802.3bt.<br>**Manager – Extensions:**<br>In the Device Editor on tab “Alarms > Global Alarms” the maximum value behind edit field “PoE Input Power Limit (W)” has been increased to 1000. Moreover, all default values on this tab have been removed for consistency. | ✓ | ✓ | ✓ |
| [from V7.01md]<br>New alarm destination types have been added to the Alarm Destination Table to show live Syslog messages in CLI consoles (“CLI Syslogs”). With this setting for each console type (Telnet, SSH or V24) the alarms to be shown in the respective CLI console when they occur can be configured.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Alarms > Alarm Destinations", the new destination types “Telnet CLI Syslog”, “SSH CLI Syslog” and “V.24 CLI Syslog” have been added to the Alarm Destination Table. | ✓ | ✓ | ✓ |
| [from V7.01nm]<br>Only applies to Desk and Industrial switches with PoE adapter:<br>The function of the yellow port LED has been extended in case of configuring it to “Show PoE Setup”:<br>Yellow LED lights continuously: PoE is activated, but no PoE-compatible end device has been detected<br>Yellow LED blinks: A PoE compatible end device has been detected and the PoE voltage is switched through | ✓ | ✓ | |
| [from V7.02B]<br>Support for the following office switch type has been implemented:<br>97 XGigaSwitch DICE 8TP 2SFP+ | ✓ | | |
| **Firmware – Security:** | | | |
| [from V7.01bv]<br>Only applies to switches with management hardware HW5:<br>The HTTPS server certificate has been extended from 2048 to 3072 bit. (RSA, 3072 Bit Key, SHA-256). | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.01bw]<br>Only applies to switches with management hardware HW5:<br>RADIUS Change of Authorization (CoA) has been added. CoA allows administrators to change authentication, authorization and accounting (AAA) attributes of a session, after it is authenticated.<br>**Manager – Extensions:**<br>In the Device Editor CoA support has been added:<br>- On tabs “State > Global+Link State” and “State > MAC+Security State” new states have been added to columns “Link States” and “Security States”<br>- On tab “State > Radius State” the states of CoA Clients 1 to 4 have been added.<br>- On tabs “Port Setup > Port <n> [<port description>], a new state has been added to “Admin State”<br>- A new tab “Security > RADIUS CoA” to enter CoA configuration parameters has been added. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |

| | | | |
|---|---|---|---|
| [from V7.01cg]<br>Only applies to switches with management hardware HW5:<br>Support for the vendor-specific RADIUS attribute Fabric Attach (FA) VLAN-I-SID has been added for IEEE802.1x and MAC-based RADIUS authentication. If FA VLAN-I-SID is configured in the RADIUS Global Authentication settings, the VLAN-ID / I-SID pair received with the Access Accept response is added to the VLAN Table, and the VLAN-ID is set as Default VLAN for the corresponding port.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Security > RADIUS Global Auth." Option "Fabric Attach with VLAN-ID and SPBM I-SID" been added to field 'VLAN attribute'. | ✓ **HW5** | ✓ **HW5** | ✓ |
| [from V7.01cj]<br>Only applies to switches with management hardware HW5:<br>Storm Protection has been added to prevent the switch from operating to fully load by unintentional or malicious packet storms. For this purpose, the number of received packets for multicast, broadcast or flooded unicast packets is limited.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Global." Options " Storm Protection Multicast (packets per second)", "Storm Protection Broadcast (packets per second)" and "Storm Protection Flooded Unicast (packets per second)" have been added to the new group "Storm Protection Setup". | ✓ **HW5** | ✓ **HW5** | ✓ |
| [from V7.01ea]<br>Only applies to switches with management hardware HW5:<br>Support for two new Aginode vendor-specific attributes (VSAs) for extended VLAN port configuration on RADIUS Access-Accept responses has been added. With these VSAs a list of VLAN-IDs and a new Trunking Mode can be set for a port via RADIUS server after successful authentication.<br>**Manager – Extensions:**<br>In the Device Editor on tab "RADIUS Global Auth.", on field "VLAN attributes" the option "AGINODE Vendor-Specific with VLAN-ID" has been renamed to "AGINODE Vendor-Specific VLAN attributes". | ✓ **HW5** | ✓ **HW5** | ✓ |
| [from V7.01km]<br>Split old combined Port Security Mode into two new separate settings "Security Mode" and "Allowed MAC Addresses" and extended number of allowed MACs to 30.<br>**Manager – Extensions:**<br>In the Device Editor support for the new Port Security has been added:<br>- On tab "Port Setup > Port n [<Port description>]", new pure Security Modes, a new edit field "Allowed MAC Addresses" and a button to edit up to 30 MAC addresses for the Security Modes "Manual" and "Vendor" in a dialog have been added.<br>- On tab "State > MAC+Security State", new pure Security Modes have been added to column "Security Mode", and columns "Used/ Allowed MAC Addresses" and "All MAC Addresses" with buttons to show all MAC addresses and states of a port in a dialog have been added.<br>In the Device List, column "Port Security Setup" the new pure Security Modes in combination with the number of allowed MAC addresses have been added. | ✓ | ✓ | ✓ |
| [from V7.01kq]<br>If Security Mode "IEEE802.1X Supplicant with MD5 Challenge" is enabled on a port, this port does not forward any other traffic now, until the security state of the port is set to "Port Authenticated". | ✓ | ✓ | ✓ |
| [from V7.01mk]<br>Port Security MAC Flapping detection has been added. If a MAC address is detected on a userport, which has already been learned or manually configured on another userport ("MAC Flapping"), the relevant port is disabled, or only a periodic alarm is sent.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Security > Security Setup", group "Portsecurity Global Setup" a dropdown-list "Portsecurity MAC Flapping Action" has been added. | ✓ | ✓ | ✓ |
| [from V7.01nu]<br>For TACACS+ Authorization the *Cisco* attribute "priv-level" is now also accepted from the TACACS+ server. However, if *Aginode* attribute "nx-access" is also specified, this attribute has higher priority.<br>*Cisco* attribute "priv-level" must be configured as follows:<br>- priv-level < 15 user has read/only access (identical to: nx-access = "NX-ACCESS-RO")<br>- priv-level ≥ 15 user has read/write access (identical to: nx-access = "NX-ACCESS-RW") | ✓ **HW5** | ✓ **HW5** | ✓ **HW5** |
| **Firmware – SNMP:** | | | |
| [from V7.01ac]<br>Requests to portPoeCurrent and portPoePower cause timeout | ✓ | ✓ | |
| **Firmware – Redundancy:** | | | |
| [from V7.02C]<br>HSR / PRP - Coupling has been implemented<br>**Manager – Extensions:**<br>In the Device Editor on tab "Redundancy > HSR / PRP", group "HSR / PRP – Global Setup" has been extended. | ✓ | ✓ | |
| **Firmware – Bug Fixes:** | | | |
| [from V7.01bc]<br>When writing the running CLI configuration with/without all parameters to the switch and the user was logged in via CLI console, the CLI console showed several parser errors and the received configuration. | ✓ | ✓ | |
| [from V7.01bc]<br>The CLI console showed "%Error: Unknown command" under certain circumstances when the prevision session was logged off by closing the Putty window with the close-button and a command was entered. | ✓ | ✓ | |
| [from V7.01bd]<br>Setting the gateway not in the scope of network mask of management interface blocked the default route That led to blocking of sending of the IP broadcast packets | ✓ | ✓ | |
| [from V7.01bd]<br>Portsecurity ageing time and Portsecurity ageing time for Allowed MACs Overflow Address also applies for Radius allow one, two and three MAC Addresses. | ✓ | ✓ | |
| [from V7.01be]<br>TACACS+ user (client) and password was limited to 64 characters. | ✓ | ✓ | |
| [from V7.01bg]<br>EEE immediately queues response was implemented. | ✓ | ✓ | |
| [from V7.01bh]<br>Clear RADIUS server state | ✓ | ✓ | |
| [from V7.01bi]<br>Spanning Tree alarms show current Root Bridge and Prio | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V7.01bu]<br>SCP file transfer and close sessions clean ups | ✓ | ✓ | |
| [from V7.01bw]<br>Use secure HTTP Header | ✓ | ✓ | |
| [from V7.01cc]<br>If Local Logging Mode was set to “Stop logging on overflow”, old log entries in the local log were overwritten anyway. | ✓ | ✓ | |
| [from V7.01ch]<br>If SNMPv1/v2/v3 Trap was activated as Alarm Destination, the switch rebooted repeatedly under certain circumstances. | ✓ | ✓ | |
| [from V7.01ci]<br>The total operation time was not shown correctly if this time was greater than one year. | ✓ | ✓ | |
| [from V7.01ck]<br>When a port was disabled by Loop Protection (link type “Userport with active Loop protection”), the port admin state in LANactive Manager was not set to "Disabled by Loop protection". | ✓ | ✓ | |
| [from V7.01cl]<br>Only applies to switches with management hardware HW5:<br>On Web interface Local Accounts was shown in the web menu (tab tree) with a delay of 5 seconds, if the user was logged in as admin. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.01cl]<br>Only applies to switches with Head PoE+ Adapter Rev.A:<br>When showing the PoE status in CLI with command “show poe”, the number of PoE pairs reported by the powered device (PD) was always 0. | ✓ | ✓ | |
| [from V7.01co]<br>On Web interface, webpage “Switch Setup” the DHCP parameters were not shown correctly, if DHCP was enabled an DHCP parameters had been received from the DHCP server.<br>For HW5 switches the DHCP parameters except DHCP Server Address were not shown at all.<br>For HW3 switches the DHCP Server Address was shown twice, but with different label. | ✓ | ✓ | |
| [from V7.01co]<br>An inconsistency with the minimum password length for local accounts has been removed. If the password strength checker was disabled, it was possible to set the minimum password length to value smaller than 8, although this parameter is only used for the password strength checker. | ✓ | ✓ | |
| [from V7.01cp]<br>Only applies to switches with management hardware HW3:<br>For HW3 Office GigaSwitches with special PoE head, PoE was not detected and activated. | ✓<br>**HW3** | | |
| [from V7.01cr]<br>On CLI console it was not possible to ping the switch’s own IP address. | ✓ | ✓ | |
| [from V7.01cr]<br>On Web interface, webpage “Queue Setup IEEE 802.1p” and "Alarm Output Setup" message "Set successful" was shown, even if nothing had been changed. | ✓ | ✓ | |
| [from V7.01cr]<br>Only applies to HW5 Office switches with SD card inserted:<br>When writing the configuration via LANactive Manager and SCP or PSCP, reading back the configuration often failed with error: “FATAL ERROR: Remote side unexpectedly closed network connection”. | ✓<br>**HW5** | | |
| [from V7.01da]<br>Only applies to switches with management hardware HW5:<br>Sometimes no IPv6 was assigned if IPv6 Access Mode was set to “DHCPv6”. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.01db]<br>Only applies to iSwitches with PoE++ Adapter Type IEEE802.3bt:<br>If one or more PoE managers on the PoE++ adapter were damaged or inaccessible, PoE was disabled completely or PoE values for connected PoE device were shown for the wrong ports.. | | ✓<br>**HW5** | |
| [from V7.01dd]<br>If Port Security Mode "IEEE 802.1x allow all MAC addresses" and RADIUS Startup VLAN-ID "Startup VLAN-ID Block Rx option" were configured on a port and first MAC address is authenticated, RX traffic for all other MAC addresses was still blocked. | ✓ | ✓ | |
| [from V7.01ea]<br>When changing the Trunking Mode from 'Disabled' to 'IEE802.1q' or 'No Tag' and back to 'Disabled', under some circumstances also packets were sent which were not part of the Default- or Voice-VLAN of the respective port. | ✓ | ✓ | |
| [from V7.01eo]<br>Only applies to switches with management hardware HW5:<br>When executing CLI command “show run” multiple times (e.g. by running script or batch file), error message “Internal Warning Code=109" (file system full) was written repeatedly to Syslog. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.01eq]<br>Only applies to switches with management hardware HW5:<br>Checksum of Customer Default/Reboot Configurations was swapped compared to switches with management hardware HW3. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.01fh]<br>When changing the Default VLAN or Voice VLAN', under some circumstances also packets were sent which were not part of the new Default- or Voice-VLAN of the respective port. | ✓ | ✓ | |
| [from V7.01fh]<br>An IP phone connected to a port of the switch configured with a Voice-VLAN never received an IP address from the DHCP Server. | ✓ | ✓ | |
| [from V7.01ks]<br>The space key in CLI command "show mac-address-table dynamic" did not work correctly when there were more than 20 MAC addresses in the MAC Address Table. | ✓ | ✓ | |
| [from V7.01ks]<br>Only applies to industrial switches with management hardware HW3:<br>In the MAC Address Table under some circumstances static IPv6 multicast addresses were shown. | | ✓<br>**HW3** | |
| [from V7.01kz]<br>If TACACS+ Authentication and CLI Command Authorization was enabled, the CLI prompt is not shown after every command call. | ✓ | ✓ | ✓ |
| [from V7.01mx]<br>Only applies to industrial switches with management hardware HW5 and HW3 16-Port switches with certain PoE adapters:<br>After reboot or reset of the switch PoE was not always available on all TP-ports that support PoE. | | ✓ | |

| | | | |
|---|---|---|---|
| [from V7.01nn]<br>The strings of LLDP-MED location types (Building, Unit, Place Type) and Fabric Attach Authentication Key were corrupted under some circumstances. | ✓ | ✓ | ✓ |
| [from V7.01no]<br>Only applies to switches with management hardware HW5:<br>If the V24/Telnet Authentication Mode was set to "TACACS+ first, then local" and TACACS+ authentication failed because of a timeout ("TACAS+ Server(s) down"), then the local password was shown in cleartext. | ✓<br>**HW5** | ✓<br>**HW5** | ✓<br>**HW5** |
| [from V7.01nq]<br>Some command parameters in CLI show commands were cut off under some circumstances. | ✓ | ✓ | ✓ |
| [from V7.01nu]<br>TACACS+ Authorization on login into SSH/Telent/V.24 CLI console was handled differently.<br>Now, at least one of the attributes "nx-access" (*Aginode*) or "priv-level" (*Cisco*) must be specified on the TACACS+ server. Otherwise Authorization fails consistently on all types of CLI consoles. | ✓<br>**HW5** | ✓<br>**HW5** | ✓<br>**HW5** |
| [from V7.01nu]<br>If a TACACS+ server IP-address for Authentication, Authorization or Accounting (AAA) was added and removed again later on, AAA requests were still sent to the removed IP address. | ✓<br>**HW5** | ✓<br>**HW5** | ✓<br>**HW5** |
| [from V7.01nu]<br>In the V.24 console the CLI command "show log" caused the switch to reboot if the Local Syslog was to long (more than approx. 600 entries). | ✓ | ✓ | ✓ |
| [from V7.02B]<br>Problems while applying customer pre-configuration in factory have been resolved. | ✓ | ✓ | |
| [from V7.02B]<br>Only applies to switches with management hardware HW5 and SD card inserted:<br>If the configuration was saved repeatedly within a short time, e.g. by entering multiple set commands in the CLI console, the switch hanged or slowed down for 20 to 30 seconds. This effect was distinct especially for HW5 7-Port Office GigaSwitches. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V7.02B]<br>Only applies to 16-Port iSwitches with management hardware HW3:<br>On SFP ports no link could be established, neither for SFPs with 1000Mbit/s nor for SFPs with 100Mbit/s. | | ✓<br>**HW3** | |
| [from V7.02B]<br>Only applies to 16-Port iSwitches with management hardware HW3 and 10-Port XGigaSwitches with management hardware HW5:<br>The green and yellow port LEDs didn't blink according to the configuration settings. | ✓<br>**HW5** | ✓<br>**HW3** | |
| [from V7.02B]<br>Cisco phones did not accept the Voice VLAN that was assigned by Aginode switches via CDP. | ✓ | ✓ | |

## 2.4. Release V6.04

### 2.4.1. Release V6.04ZC

| **Switch family →** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family HW3→** | **HW3-Fxx-Pxx-OFFICE** | **HW3-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V6** |
| **Firmware family HW5→** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V6** |
| **Manager – Basic Features:** | | | |
| [from V6.04Z]<br>A function to search for MAC Address in the MAC Address tables of all currently shown Devices has been added. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>A new feature has been added, which allows the user to set up a time scheduled configuration. The controller will send a configuration file at a specific time of day to a device and restore the old configuration after a given time span. | | | ✓ |
| [from V6.04Z]<br>Stand-Alone:<br>The grid in the Discovery-Mode dialog has been changed, to have functionalities like filtering and grouping available. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>A function to export current Device-List as .xml-File has been added. This file can be imported by other clients or even the Stand-Alone version. | | | ✓ |
| [from V6.04Z]<br>Page "CLI Scripting" has been added to Device-Editor → Management. On this page the device's script file can be read, edited and sent back to the device. The function to send a script file to any device has also been added to Templates → Copy Master-Config and Configuration Templates to checked Devices simultaneously in the main menu. The function read script file from the devices inside the current Device-List has been added to "Edit" in the main menu. | | | ✓ |
| [from V6.04Z]<br>Device-List columns 'Script File Size' and 'Script File Checksum' has been added. These columns indicate whether a script file is stored and running on the device. | | | ✓ |
| [from V6.04Z]<br>'Offline Switches Timeout' has been added to 'General Settings → Import from file'. If a device is offline for more than this amount of days, it will be removed from the target Device-List. | | | ✓ |
| [from V6.04Z]<br>If the IP Address of a Device is updated during Zero Touch Configuration, this Address will be updated in the database on the next Zero Touch Configuration paket. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V6.04Z]<br>The User Management now shows the state of all users, meaning if they are online or offline. It is also possible for administrators to kill any user session except their own if necessary. | | | ✓ |
| [from V6.04Z]<br>In the Device-Editor a new tool strip item 'Database file → Save Config as' has been added. By clicking on this menu item it is possible to save the current configuration under a specific name for a better identifying when loading it back from the config history. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>Option to enable usage of SSL for sending E-Mails has been added to the Settings menu. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>It is now possible to run the time scheduled device import multiple times a day. Also, a button to run the import immediately has been added to the settings menu. | | | ✓ |
| [from V6.04Z]<br>Temperature column has been added to the Device-List | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>Zero-Touch-Configuration now supports firmware downgrades. | | | ✓ |
| [from V6.04Z]<br>Column "Last Login" has been added to User Management. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>From now on it is possible to change the default preferences path during the setup. Under this path the LANactive Manager.config file is stored. | | | ✓ |
| [from V6.04Z]<br>Group row headers of any grid now contain the number of grouped items. | | | ✓ |
| [from V6.04Z]<br>Column "Time from time server" has been added to the Device-List, showing the time the switch has received from the SNTP server. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>E-Mail notifications of Syslog- and SNMP-Message will be queued and sent after 30 seconds to reduce the amount of Email-Notifications. | | | ✓ |
| [from V6.04Z]<br>New HW5 P10 Office switch has been added to Zero Touch Configuration settings. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V6.04Z]<br>Master-Configs could overwrite the IP Address of a switch, if the correspondent check box is checked but no .csv-file is selected. | | | ✓ |
| [from V6.04Z]<br>Device-Editor → VLAN Table → Fabric Attach Authentication Key was missing in the master configuration. | | | ✓ |
| [from V6.04Z]<br>Device-Editor → VLAN Table →When changing VLAN Table Mode from 64 to 256 VLANs, SPBM I-SID is now saved inside the grid. | | | ✓ |
| [from V6.04Z]<br>When opening a second Master-Config, instead of being opened in a new window the first Master-Config window was overwritten. | | | ✓ |
| [from V6.04Z]<br>When closing a Device-Editor the question whether the configuration should be saved is now only shown when any changes have been made. | | | ✓ |
| [from V6.04Z]<br>On Device-Editor page 'VLAN Table', the buttons 'Select ALL Tag', 'Select ALL Untag' and 'Not Allowed' were not working correctly. | | | ✓ |
| [from V6.04Z]<br>When set to hybrid mode, after changing the default VLAN the VLAN Tagging of all VLANs has been reset to 'not allowed'. | | | ✓ |
| [from V6.04Z]<br>During import of devices from external file, double MAC addresses where not deleted if two existing devices switch their IP addresses. | | | ✓ |
| [from V6.04Z]<br>Zero-Touch-Configuration can be partially used in Evaluation version. | | | ✓ |
| [from V6.04Z]<br>Using "Read CLI-Config of checked Devices into local database file (with all parameters) simultaneously" and TFTP caused the LANactive Manager to read the binary config instead. This bug is now fixed. Additionally, the LANactive Manager will always use SCP for reading this file, because the firmware does not support reading this file with TFTP. | | | ✓ |
| [from V6.04Z]<br>When importing Device-List to Database, existing switches where not skipped and exists multiple times in the database afterwards. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>The Repair-Button has been removed from the Setup, because this option reinstalls all option with default values only. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>Switch locks where not deleted in every case from database after Device-Editor has been closed. | | | ✓ |
| [from V6.04Z]<br>When changing the name of a switch using master configuration with an additional csv-file, the log massages of the progress where not written. | | | ✓ |
| [from V6.04Z]<br>When updating the firmware of any switch, the LANactive Manager did not wait long enough for the switch to start flashing. This could lead to an early finish of the process with wrong error messages. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V6.04Z]<br>On some tabpages in the Device-Editor the vertical scroll bars where missing when not using fullscreen mode. | | | ✓ |
| [from V6.04Z]<br>Generating IP address ranges for Layer-3-Autodiscovery didn't work correctly in the Stand-Alone version. This bug is now fixed. | | | ✓ |
| [from V6.04Z]<br>Username/Password dialog for firmware update was not formatted correctly on Windows 10. | | | ✓ |
| [from V6.04Z]<br>When creating a controller log message, instead of trying to find the current IP address, 'Controller' is written to the 'Sender IP Address' field. | | | ✓ |
| [from V6.04Z]<br>After opening the Device-Editor it could happen that the device is marked light green and some values are marked yellow even if they didn't change. This bug is now fixed. | | | ✓ |
| [from V6.04Z<br>Temperature column in the Device-List was not sorted correctly. This is now fixed | | | ✓ |
| [from V6.04Z]<br>When Client and Controller are running on the same machine, a message box saying that the file is already existing popped up every time a configuration file was uploaded to the controller. This issue is now solved. | | | ✓ |
| [from V6.04Z]<br>A bug is fixed which caused the LANactive Manager to send an additional UDP Request to the switch after closing the Cable Diagnostic Dialog. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>After saving the client preferences the settings were not updated if the user just logged out and in again instead of restarting the application. This is now fixed. | | | ✓ |
| [from V6.04Z]<br>Error message boxes are not hidden behind their parent form anymore. | | | ✓ |
| [from V6.04Z]<br>In Layer 2 Autodiscovery sometimes random cells were marked green. This does not happen anymore. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>Log-Messages were not correctly formatted when a switch was using SNTP Time Client. | | | ✓ |
| [from V6.04Z]<br>Device-Editor -> VLAN Table -> Delete VLAN Id was not working with Firmware Versions below V6.04N. | | | ✓ |
| [from V6.04Z]<br>Updating Master-Config using "Device-Editor -> Template -> Update existing Master-Configs with new firmware features of this device" could breaks Master-Configs created with firmware version V6.01 or below. | | | ✓ |
| [from V6.04Z]<br>On Device-Editor page Security → Security Setup, the Vendour OUI textboxes were not enabled if Voice VLAN Authentication Mode was set to "Bypass Authentication for three Vendor Addresses" | | | ✓ |
| [from V6.04Z]<br>On Device-Editor page Security → TACACS+ Accouting the master checkbox for the Accounting Mode was missing and has been added. | | | ✓ |
| [from V6.04Z]<br>Adding items to Predefined Devices list took extremely long on large lists due to wrong item validation. This bug has been fixed. | | | ✓ |
| [from V6.04Z]<br>Client/Controller:<br>Setting Preferences → Controller Poll Interval to zero caused the Manager to crash. This bug has been fixed. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V6.03ah]<br>Only applies to switches with management hardware HW5:<br>CLI Scripting to trigger the execution of CLI commands on certain system events has been added. Based on a pre-defined event, a list of CLI commands will be started. The list of commands assigned to a certain event is called *CLI Script*. A pre-defined event can be a status change of a port or functional input, or a time-based event. All CLI Scripts to be executed on a pre-defined event are included in a *CLI Script file* which is transferred to / from the switch via SCP.<br>**Manager – Extensions:**<br>In the Device Editor the tab "CLI Scripting" has been added. On this tab the CLI Script file can be edited in the textbox "Script File Content". By pressing buttons "Write Script to Device and Database file" and "Read Script from Device" the CLI Script file can be written to / read from the switch, respectively. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.03eb]<br>Support for the following cable duct switch type has been implemented:<br>78 (Gigaswitch V5 2TP(PD-F+) SFP-VI) | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03fb]<br>The functionality of the IEC61850 "Power Supply Alarm" (object LPHD1.PwrSupAlm.stVal) has been extended. This alarm is now triggered if either one of the internal supply voltages 2.5 or 3.3 V, or one of the external power supply voltages S1 or S2 is out of range. | ✓ | ✓ | |
| [from V6.03fw]<br>Support for Reset Action "Reboot with Factory Default" in LANactive Manager has been added, according to CLI and WEB. Before, in LANactive Manager only the Reset Action "Reboot with Factory Default (Except IP Parameters)" available.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Management > Agent" the option "Reboot with Factory Default" has been added to dropdown list "Reset Action". | ✓ | ✓ | |
| [from V6.04G]<br>The 'Flow Control' function has been disabled by factory default because the current switch chips don't need this function for proper operation. | | ✓ | |

| | | | |
|---|---|---|---|
| [from V6.04H]<br>Only applies to GigaSwitch V5 cable duct switches with PoE+ adapter Rev.B and Rev.B1:<br>If the PoE setup for a particular port is set to IEEE802.3at (PoE+ / 30W), the power negotiation is done via Layer-2 protocol LLDP-MED according to IEEE802.3at standard. Now additionally a Layer-1 negotiation via 2-event classification has be implemented. Both Layer-1 and Layer-2 negotiation are working in parallel.<br>Note: Cable duct switches with PoE+ adapter Rev.A only support Layer-2 negotiation via LLDP. This conforms to the standard as a PoE power sourcing device only needs to support one type of power negotiation (Layer-1 or Layer-2). | ✓<br>**HW5** | | |
| [from V6.04H]<br>Only applies to industrial switches with function inputs and multicolor alarm LEDs:<br>For function inputs, the corresponding status LEDs now light up in red or green depending on the setting of the function input alarm setting. | | ✓ | |
| [from V6.04H]<br>Only applies to switches with management hardware HW5:<br>Jumbo Frame support has been enabled with a maximum packet length of 9600 bytes. Even there is no IEEE standard for jumbo frames, the use of a maximum of 9000 bytes for jumbo frames is generally recommended to ensure compatibility between different switch manufacturers. Thus the allowed 9600 bytes offer enough margin for future extensions of the packet length, especially for applications with additional VLAN tags. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.04V]<br>Support for the following industrial switch type has been implemented:<br>86 (iGigaSwitch 1004 E+ SFP-4VI HW5) with hardware version 04 or higher. | | ✓<br>**HW5** | |
| **Firmware - Security:** | | | |
| [from V6.03gp]<br>For all RADIUS based port security modes the “Startup VLAN-ID” can now optionally block RX traffic from end devices. This RX blocking persists until the end device is authenticated by RADIUS (via IEEE802.1X or via MAC based authentication) or the end device is moved to the ‘Guest VLAN’, ‘Inaccessible VLAN’ or ‘IEEE802.1x Authentication Failure VLAN’. Furthermore, the RX blocking also applies to end devices in the Port Voice-VLAN.<br>**Manager – Extensions:**<br>In the Device Editor on tab “Security > Global Authentication Server Setup” the parameter “Startup VLAN-ID” has been expanded with the following modes:<br>- Unsecure VLAN-ID (Block RX traffic to VLAN for unauthorized MACs)<br>- Port Default VLAN-ID (Block RX traffic to VLAN for unauthorized MACs) | ✓ | ✓ | |
| [from V6.03gv]<br>In order to maximize the resistance against network attacks on the Linux operating system of the Switch, the included Dropbear SSH server package has been completely removed from the firmware file system. Because this server was not running during switch operation, it was a very low-level security issue. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.04D]<br>For port security mode “IEEE802.1X allow all MAC addresses” the “IEEE802.X RADIUS MAC Bypass” function has been implemented. If the Bypass is activated, only the first detected MAC address is authenticated after an IEEE802.1X timeout. If the RADIUS server confirms the MAC address, the port is switched through. Important: All subsequent detected MAC addresses are ignored for authentication, even in the event that the address detected first was rejected by the RADIUS server. | ✓ | ✓ | |
| [from V6.04D]<br>If the "VLAN table mode" is set to "Dynamic", and also the Spanning Tree is activated, VLAN 1 is not deleted, even if VLAN 1 is not defined for any port VLAN or any another global VLAN. This is necessary because VLAN 1 is required for eventually connected PVST devices (Per-VLAN Spanning Tree). | ✓ | ✓ | |
| [from V6.04N]<br>A new parameter called "RADIUS Inaccessible Voice VLAN-ID" has been implemented. This parameter defines the Voice VLAN-ID in the case that no RADIUS server is reachable.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "VLAN > VLAN Setup > VLAN Security Setup" the parameter "RADIUS Inaccessible Voice VLAN-ID“ has been added. Moreover, if no RADIUS server is reachable, on tab “Global+Link State” in column “Active Voice VLAN” the state “<Inaccessible-VLAN>” is displayed behind the Voice VLAN. | ✓ | ✓ | ✓ |
| [from V6.04Q]<br>Three new parameters for the vendor addresses (Vendor OUIs), and a new option "Bypass Authentication for three Vendor Addresses" have been implemented for parameter “Voice VLAN Authentication Mode”. If this option is selected, for all ports on which Radius or IEEE802.1X based authentication is configured, the MAC addresses in a Voice VLAN containing the configured Vendor OUIs are bypassed without authentication.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Security Setup > Port Security Global Setup” option "Bypass Authentication for three Vendor Addresses" has been added to parameter “Voice VLAN Authentication Mode”, and the parameters “Vendor OUI 1” to “Vendor OUI 3” have been added for this new option. | ✓ | ✓ | ✓ |
| **Firmware – SNMP:** | | | |
| [from V7.01ac]<br>Requests to portPoeCurrent and portPoePower cause timeout | ✓ | ✓ | |
| [from V6.03cd]<br>The port trunking mode "hybrid (4)" has been added to AGINODE Private SNMP MIB object portTrunkingMode. | ✓ | ✓ | |
| [from V6.03bv]<br>Reading and writing the configured VLAN membership of all ports via the SNMP Q-BRIDGE-MIB has been implemented. For this purpose, the existing SNMP objects dot1qVlanStaticEgressPorts and dot1qVlanStaticUntaggedPorts have been extended. | ✓ | ✓ | |
| [from V6.03bv]<br>Reading the active VLAN membership of all ports via the SNMP Q-BRIDGE-MIB has been implemented. For this purpose, the existing SNMP objects dot1qVlanCurrentEgressPorts and dot1qVlanCurrentUntaggedPorts have been extended. | ✓ | ✓ | |
| [from V7.01ac/V6.04Q]<br>Requests to portPoeCurrent and portPoePower cause timeout | ✓ | ✓ | |
| **Firmware – Redundancy:** | | | |

| | | | |
|---|---|---|---|
| [from V6.03gr]<br>In order to avoid network loops in spanning tree topologies, the internal time window for the automatic detection of edge ports has been extended. This makes the topology more stable if the port does not receive the first BDPUs shortly after a Link-Up. | ✓ | ✓ | |
| [from V6.04E]<br>In order to avoid network loops in MRP ring topologies, the internal timeouts for missing MRP BPDUs has been modified. This makes the topology much more stable during configuration changes of the switches. | ✓ | ✓ | |
| [from V6.04T]<br>New parameter called "Spanning Tree Loop Guard" has been implemented. Enabling the Loop Guard prevents a blocking port to move to the forwarding state because of lost BPDUs and thus avoids loops in the network. See manual for a detailed description.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Redundancy > Spanning Tree" the parameter "Loop Guard enable“ has been added. | ✓ | ✓ | ✓ |
| [from V6.04T]<br>New parameter called "MRP Loop Guard" has been implemented. Enabling the Loop Guard prevents a blocking port to move to the forwarding state because of lost echo packtes and thus avoids loops in the network. See manual for a detailed description.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Redundancy > MRP" the parameter "Loop Guard enable“ has been added. | ✓ | ✓ | ✓ |
| [from V6.04V]<br>New parameter called "Spanning Tree Loop Guard Timeout" has been implemented. If the Spanning Tree Loop Guard is triggered, this is the maximum time in minutes after which the Loop Guard is temporarily deactivated if no BPDUs are received. After a deactivation time of 10 seconds, the Loop Guard is reactivated. See manual for a detailed description.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Redundancy > Spanning Tree" the parameter "Loop Guard timeout“ has been added. | ✓ | ✓ | ✓ |
| **Firmware – Bug Fixes:** | | | |
| [from V6.03bv]<br>The Voice VLAN ID could not be set by SNMP object portVoiceVlanId if Trunking Mode was ‘Disabled’. This problem has been fixed. | ✓ | ✓ | |
| [from V6.03cn]<br>Only applies to switches with management hardware HW5:<br>If the port security setting “Shutdown if no Link” was set to “Check Link permanently delayed”, the port was erroneously disabled after rebooting the switch. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03eq]<br>IPv6 access to switch management via SFP ports doesn’t work. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03ew]<br>Only applies to GigaSwitch V5 cable duct switches with PoE+ adapter Rev.B and Rev.B1:<br>Each time the configuration was written to the switch via LANactive Manager, the PoE voltage for the attached PoE end devices was interrupted for a short period. | ✓<br>**HW5** | | |
| [from V6.03ez]<br>If the switch management received a ping request with routing parameters included, the management might hang up. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03ez]<br>If both Spanning Tree and CDP were enabled, the “Active Loop Protection” feature for user ports may not work properly. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03fx]<br>The gateway IPv6 address for DHCPv6 was not shown on CLI command 'show dhcp'. | ✓ | ✓ | |
| [from V6.03fx]<br>Only applies to switches with management hardware HW5:<br>In rare cases the switch could hang up the IPv6 Access Mode was set to DHCPv6. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03gh]<br>Only applies to switches with management hardware HW5:<br>Activating Multicast parameters "Multicast snooping enable" and "IGMP Querrier enable" in parallel could make the switch unreachable and unusable under certain circumstances. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.03gh]<br>Only applies to switches with management hardware HW3:<br>IGMP queries sent by HW3 switches were not detected and handled correctly by HW5 switches Multicast features enabled. | ✓<br>**HW3** | ✓<br>**HW3** | |
| [from V6.04A]<br>Only applies to industrial switches with HSR uplink ports:<br>If the HSR SFP ports were equipped with 100 Mbit/s SFPs and the link of the first HSR port was lost, then the communication via the second HSR port was also interrupted. | ✓ | ✓ | |
| [from V6.04C]<br>Only applies to switches with management hardware HW5:<br>Under certain circumstances the PoE voltage was switched off after reboot or firmware update. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.04F]<br>Only applies to switches with management hardware HW5:<br>If the function ‘Tagging Ethertype’ was set to 9100 or 9200 (Q-in-Q Function), the management interface of the switch was not accessible under certain circumstances. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.04F]<br>Only applies to industrial switches with 16 ports:<br>The function ‘Show Spanning Tree State’ within the LANactive Manager Switch Manager didn’t show the complete status text under certain circumstances. | | ✓ | |
| [from V6.04H]<br>Only applies to industrial switches with alarm output(s):<br>If a switch received “Remote Function Inputs Alarms” from two or more switches in the same alarm group simultaneously, the alarm output was not switched correctly under certain circumstances. | | ✓ | |
| [from V6.04R]<br>Setting the gateway not in the scope of network mask of management interface blocked the default route That led to blocking of sending of the ip broadcast packets | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V6.04R]<br>Portsecurity ageing time and Portsecurity ageing time for Allowed MACs Overflow Address also applies for Radius allow one, two and three MAC Addresses | ✓ | ✓ | |
| [from V6.04R]<br>TACACS+ user (client) and password is limited to 64 characters | ✓ | ✓ | |
| [from V6.04U]<br>If EEE (Energy Efficient Ethernet) was enabled, the bandwidth of that port was limited under certain circumstances. | ✓ | ✓ | |
| [from V6.04V]<br>If SNMPv1/v2/v3 Trap was activated as Alarm Destination, the switch rebooted rarely under certain circumstances. | ✓ | ✓ | |
| [from V6.04W]<br>When changing the Trunking Mode from 'Disabled' to 'IEE802.1q' or 'No Tag' and back to 'Disabled', under some circumstances also packets were sent which were not part of the Default- or Voice-VLAN of the respective port. | ✓ | ✓ | |
| [from V6.04W]<br>If the port is set to port security mode "802.1x allow one mac address", "Request Identity" EAP packages are now sent as unicast packages. Some IP phones, e.g. Avaya IP phones, only get authenticated if they receive this request as unicast. | ✓ | ✓ | ✓ |
| [from V6.04X]<br>On internal Pre-configuration, the CLI command to set Port VLAN Isolation was not accepted. | ✓ | ✓ | |
| [from V6.04X]<br>On internal Pre-configuration, the CLI command to set the link type for Loop Protection was accepted but not saved. | ✓ | ✓ | |
| [from V6.04Y]<br>When less than four RADIUS Server IP Addresses were defined for RADIUS Global Authentication and the Server Request Algorithm is set to "Parallel", RADIUS authentications caused alarms that were shown in the Device-List, column "Alarms" for the corresponding switch. | ✓ | ✓ | |
| [from V6.04Z]<br>Only applies to certain switch types with management hardware HW5 and certain PoE adapters:<br>After reboot or reset of the switch the PoE adapter was not always detected. Hence, no PoE was available on the switch. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.04Za]<br>Problems while applying customer pre-configuration in factory have been resolved. | ✓ | ✓ | |
| [from V6.04ZC]<br>If one device connected to the switch (e.g. an IP-phone) was authenticated via IEEE802.1X, and another device connected to the first device was authenticated via RADIUS, the IEEE802.1X learned MAC addresses could disappear from the MAC table after a random time. | ✓ | ✓ | |

## 2.5. Release V6.02

## 2.5.1. Release V6.02O

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family HW3➔** | **HW3-Fxx-Pxx-OFFICE** | **HW3-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V6** |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V6** |
| **Manager – Basic Features:** | | | |
| [from V6.02C]<br>Communication with switches using only IPv6 is now fully implemented. | | | ✓ |
| [from V6.02C]<br>Before starting Layer 2 discovery mode, the user can choose between a particular or all available network interfaces. | | | ✓ |
| [from V6.02C]<br>Another type of Inventory-List including MAC Address and LLDP Information can be created from the Inventory-Menu. | | | ✓ |
| [from V6.02C]<br>Client/Controller: A settings menu has been added to the Database Management. Hereby the user can configure the controller settings, like polling, UDP or notification settings. | | | ✓ |
| [from V6.02C]<br>Client/Controller: Zero-Touch-Configuration has been added to the LANactive Manager Controller. New Devices inside the network (Firmware Family HW5 and Firmware Version V6.xx) can be discovered, updated, configured and added to the database automatically. Therefor different firmware and configuration files can be uploaded to the controller. It is also possible to create a list which assigns different configuration files to specific devices to have them be configured individually. | | | ✓ |
| [from V6.02C]<br>Client/Controller: The Controller is now able to receive Syslog and SNMP Trap Messages and to store them in the database. SNMP Traps are translated immediately. Additionally, the controller logs own types of messages, for example when a device went offline. | | | ✓ |
| [from V6.02C]<br>Client/Controller: The Controller now supports sending E-Mails. E-Mails can contain information about new devices added by Zero-Touch-Configuration, received Log Messages or notifications from the Controller itself. Therefore, E-Mail accounts for sending and retrieving this E-Mails and the SMTP Server to use for E-Mail communication must be configured using the Settings Menu. | | | ✓ |
| [from V6.02C]<br>Client/Controller: The Controller now supports time scheduled importing of device from a .csv file into the database, which is created by any third-party software. The devices will be added into a new device list named after the file to import from and a category tree will be created depending on the location. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V6.02C]<br>All grid views now support filtering by specific columns. | | | ✓ |
| [from V6.02C]<br>Client/Controller Setup: If previous version is installed, old preferences like data folders or database settings will be adopted. | | | ✓ |
| [from V6.02C]<br>Client/Controller Setup: Administrator user have access to all Device-Lists without having them explicitly assigned. | | | ✓ |
| [from V6.02C]<br>Parameter 'Automatic Powersave' from 'Port Setup' and page 'Time Client' → 'Powersave Setup' have been removed from the Device-Editor, because 'Port Setup' → 'Energy Efficient Ethernet' has been added. | | | ✓ |
| [from V6.02C]<br>Inside the Device-Editor the number of checked master checkboxes is shown in the tree view for each page. The parent node contains the sum of all child nodes. | | | ✓ |
| [from V6.02C]<br>Device-List column 'Backup Firmware Version' has been added. This column shows the version of the backup firmware and the number of the partition where it is stored on. | | | ✓ |
| [from V6.02C]<br>On page 'Device-Info' inside the Device-Editor parameter 'Backup Firmware Version / Partition' have been added. This parameter shows the version of the backup firmware and the number of the partition where it is stored on. These parameters are also shown in the 'Live Information'. | | | ✓ |
| [from V6.02L]<br>Client/Controller:<br>The file path, which is used by the Controller to store uploaded config files, is now configurable on page 'Settings → General Settings'. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V6.02D]<br>Only applies to switches with management hardware HW5:<br>The Manager Device-List column "Backup Firmware Version" shows wrong text under certain circumstances. | | | ✓ |
| [from V6.02D]<br>In Device Editor the menu item "Edit > Write Config to fixed IP 172.23.44.111" used IP of the current switch instead of fixed IP. | | | ✓ |
| [from V6.02E]<br>Client/Controller:<br>A Bug has been fixed which caused an overflow exception while polling any device from the controller. | | | ✓ |
| [from V6.02E]<br>A Bug has been fixed which caused an error while copying old master configurations to any switch. | | | ✓ |
| [from V6.02E]<br>Error messages during switch interactions were not written to log message window. This problem has been fixed. | | | ✓ |
| [from V6.02E]<br>A Problem has been fixed which caused the firmware update via TFTP to abort at a random point of time. | | | ✓ |
| [from V6.02E]<br>A Problem has been fixed which prevented the writing of new configurations to any device when parameter "Don't save Config to Database" is set to true in preferences. | | | ✓ |
| [from V6.02E]<br>A Problem has been fixed which forced the LANactive Manager Client Predefined Devices dialog to run in an idle loop forever when cancelling the file selection for importing predefined devices from a csv file. | | | ✓ |
| [from V6.02F]<br>A bug has been fixed which caused the Device-Editor to stay in "Device Offline Mode" after a reboot action has been set on the switch. | | | ✓ |
| [from V6.02G]<br>Client/Controller:<br>Poll Engine created super-sized error log files after connection to database was lost. | | | ✓ |
| [from V6.02L]<br>Client/Controller:<br>A bug has been fixed which caused an error when the controller copied master configurations to any switch on 64bit systems. | | | ✓ |
| [from V6.02L]<br>Client/Controller:<br>Zero Touch Configuration state was not reloaded after controller update. | | | ✓ |
| [from V6.02L]<br>Client/Controller:<br>While using server-side Layer 2-Discovery, existing MAC Addresses could not be updated with rediscovered switches and their new IP Address. | | | ✓ |
| [from V6.02O]<br>Client/Controller:<br>A bug has been fixed which caused a problem during the registration of the client. | | | ✓ |
| [from V6.02O]<br>Client/Controller:<br>A bug has been fixed which caused an error while saving the controller settings because of wrong default values. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V6.01dq]<br>Access Control Lists (ACLs) for IPv4 / IPv6 Layer 3 rules and MAC Layer 2 rules have been added. ACLs can be configured as static ACLs (SACLs) or dynamically be received from a RADIUS server as dynamic ACLs (DACLs). In total maximal 64 ACLs are allowed and up to 200 rules can be assigned to one ACL.<br>**Manager – Extensions:**<br>In the Device Editor the tab "Access Control List" has been added. On this tab new ACLs and rules can be created by entering the respective CLI commands into the textbox "Access Control List Commands". | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |

| | | | |
|---|---|---|---|
| [from V6.01dv]<br>Energy-Efficient Ethernet (EEE) support has been added for HW5 switches. EEE can be enabled / disabled separately per port.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Port Setup > Port *n* [<port description>]" the checkbox "Energy Efficient Ethernet Enable" has been implemented. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.01ed]<br>TACACS+ Authentication protocol support has been added for HW5 switches.<br>This protocol is used for the following authentication tasks in the switch:<br>- Telnet authentication of Name/Password<br>- SSHv2 authentication of Name/Password<br>- V.24 authentication of Name/Password<br>- SCP authentication of Name/Password<br>**Manager – Extensions:**<br>In the Device Editor the following tabs have been added:<br>- tab "Security > TACACS+ Authentication" to configure TACACS+ Authentication<br>- tab "State > TACACS+ State" to view the TACACS+ server states<br>In the Device Editor on tab "Management > Access Global" the console authentication modes "TACACS+ only" and "TACACS+ first, then local" have been added to the following dropdown lists:<br>- "Telnet authentication mode"<br>- "SSHv2 authentication mode"<br>- "SCP authentication mode"<br>- "V.24 authentication mode" | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.01ed]<br>TACACS+ Authorization protocol support has been added for HW5 switches.<br>This protocol is used for the following authorization tasks in the switch:<br>- Telnet authorization of users for general access rights (read-write, read-only)<br>- Telnet authorization of CLI commands<br>- SSHv2 authorization of users for general access rights (read-write, read-only)<br>- SSHv2 authorization of CLI commands<br>- V.24 authorization of users for general access rights (read-write, read-only)<br>- V.24 authorization of CLI commands<br>- SCP authorization of users for general access rights (read-write, read-only)<br>**Manager – Extensions:**<br>In the Device Editor the following tabs have been added:<br>- tab "Security > TACACS+ Authorization" to configure TACACS+ Authorization<br>- tab "State > TACACS+ State" to view the TACACS+ server states | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.01ed]<br>TACACS+ Accounting protocol support has been added for HW5 switches.<br>This protocol can be used, among others, for the following tasks:<br>- Recording of the exact periods of time a TACACS+ user was active<br>- Recording of the related IP addresses<br>- Recording of the executed console commands<br>**Manager – Extensions:**<br>In the Device Editor the following tabs have been added:<br>- tab "Security > TACACS+ Accounting" to configure TACACS+ Accounting<br>- tab "State > TACACS+ State" to view the TACACS+ server states | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.01cw]<br>Show alarm in Device List, column "Alarms" of Manager for HW5 switches and TACACS+ if<br>- a TACACS+ server is unreachable<br>- there is a fail in TACACS+ authentication or authorization on a port.<br>The alarm is automatically cleared if the problem does not persist. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.01ef]<br>A new Reset Action to switch the boot partition has been added in CLI and Manager.<br>In the CLI a new reload command has been added:<br>`rel:oad b:ackup-firmware`<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Management > Agent" the Reset Action "Switch to backup firmware" has been added. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.01ef]<br>Show running and backup firmware version, and boot partition in CLI and Manager for HW5 switches.<br>In the CLI the `show info` command has been extended:<br>`Running Firmware version [Boot partition` *m*`]`<br>`Backup Firmware version [Boot partition` *n*`]`<br>where *m*, *n* = {1; 2} and *m* ≠ *n*<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Device Info" text field "Backup Firmware Version", and in Device List column "Backup Firmware Version / Partition" with the backup firmware version and boot partition has been added. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.02A]<br>Zero Touch Configuration has been implemented for HW5 switches. With this feature the configuration process and the programming of firmware upgrades can be automated. If Zero Touch Configuration is enabled, new switch configurations and firmware will automatically be provided by the LANactive Manager Controller.<br>**Manager – Extensions:**<br>In the Device Editor tab "Management > Zero Touch Configuration" has been added. This tab contains the parameters "Zero Touch Configuration Mode" and "Controller IP Address". | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.02B]<br>Extended Power Save support has been added for certain HW5 switches. Extended Power Save can be enabled / disabled separately per port.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Port Setup > Port n [<port description>]" the checkbox "Extended Powersave Enable" has been implemented. | ✓<br>**HW5** | | ✓ |
| [from V6.02D]<br>Only applies to industrial switches of type "iSwitch 742" (switch type 32 and 35):<br>The VLAN configuration is copied from port 6 and 7 to port 9 and 10 to make it easier to exchange an iSwitch 742 on site with an iGigaSwitch 1002 via a memory card. As a result, the VLAN settings of the two SFPs ports are identical after the exchange. | | ✓<br>**HW3** | |

| | | | |
|---|---|---|---|
| [from V6.02K]<br>Only applies to GigaSwitch V5 cable duct switches with management hardware HW5 and PoE+ functionality for the four front copper ports:<br>Support for PoE+ adapter Rev.B1 has been implemented. | ✓<br>**HW5** | | |
| [from V6.02M]<br>Only applies to industrial switches of type “iSwitch 542” (switch type 38):<br>The VLAN configuration is copied from port 1 and 5 to port 9 and 10 to make it easier to exchange an iSwitch 542 on site with an iGigaSwitch 1002 via a memory card. As a result, the VLAN settings of the two SFPs ports are identical after the exchange. | | ✓<br>**HW3** | |
| [from V6.02M]<br>Support for the following industrial switch type has been implemented:<br>86 (iGigaSwitch 1004 E+ SFP-4VI HW5) with hardware version 02 or higher. | | ✓<br>**HW5** | |
| **Firmware - Security:** | | | |
| | | | |
| **Firmware – SNMP:** | | | |
| [from V6.01dz]<br>SNMP support for public ENTITY.MIB, sub MIB entPhysicalTable (Entity Physical Table) according to RFC 6933 has been implemented.<br>For this purpose, the follow MIBs have been added to the set of Aginode SNMP MIBs:<br>- Entity-MIB.mib<br>- IANA-Entity-MIB.mib<br>- UUID-TC-MIB.mib | ✓ | ✓ | |
| **Firmware – Redundancy:** | | | |
| [from V6.02F]<br>If LACP is enabled, the status details are now inserted in the status packet send to the manager device list for column "Redundancy Details".<br>**Extensions in the Manager:**<br>In the Device-List the tool tip message for column "Redundancy Details" has been completed and renamed to "Redundancy and Loop Protection Details" | ✓ | ✓ | ✓ |
| [from V6.02G]<br>New parameter called "Link Aggregation Protocol Timeout" implemented. This parameter defines the timeout and send interval for LACP packets. The factory default value is set to “Slow” (in the previous firmware versions this value was fixed set “Fast”). Furthermore, the active status of the local and remote port timeout is shown with the LACP status.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Redundancy > Link Aggregation" the parameter " Link Aggregation Protocol Timeout“ has been added. | ✓ | ✓ | ✓ |
| **Firmware – Bug Fixes:** | | | |
| [from V6.01co]<br>Even a SNTP time server was configured, the first local log messages after reboot had no time stamp. This problem has been fixed. | ✓ | ✓ | |
| [from V6.02B]<br>Only applies to switches with management hardware HW5:<br>If a SFP port was equipped with an 100Mbit/s SFP, under certain circumstances the port wrongly detected a link signal, even there was no fiber connected or the SFP was removed. This problem has been fixed.<br>Note: For a stable detection of low power conditions only use SFPs with DDM functionality. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02C]<br>Entering CLI command “help” could lead to an error message instead of displaying the searched CLI commands. | ✓ | ✓ | |
| [from V6.02D]<br>Only applies to switches with management hardware HW3:<br>If the “Password encryption mode” was enabled, the CLI command “show running-config” or the Manager menu item “Read CLI config…” could lead to reboot of the switch. | ✓<br>**HW3** | ✓<br>**HW3✓** | |
| [from V6.02D]<br>Only applies to switches with management hardware HW5 and firmware version V6.01dg or higher:<br>If link aggregation redundancy was enabled, the automatic configuration of the LAG group through LACP may not work correctly. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02D]<br>Only applies to industrial switch of type “iSwitch 742” (switch type 35) with “Disable” input:<br>The output alarms M1 and M2 didn’t work under certain circumstances. | | ✓<br>**HW3** | |
| [from V6.02D]<br>Only applies to industrial switches with management hardware HW5:<br>Spanning tree was not enabled by factory default. Furthermore, the factory default settings for “Max. age/hops” and “Forward delay” were different compared to industrial switches with management hardware HW3. | | ✓<br>**HW5** | |
| [from V6.02D]<br>Only applies to industrial switches with management hardware HW5:<br>After first update to a V6.xx firmware version, the Manager Device-List column “Backup Firmware Version”, shows random wrong text under certain circumstances. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V6.02E]<br>Only applies to switches with management hardware HW3 and firmware version V5.03fx or higher:<br>If “Active Loop Protection” was enabled, a loop between two copper ports may result in a switch hang up. | ✓<br>**HW3** | ✓<br>**HW3** | |
| [from V6.02E]<br>Only applies to switches with management hardware HW5:<br>If the port security setting “Shutdown if no Link” was set to “Check Link permanently delayed”, the port was erroneously disabled after rebooting the switch. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02G]<br>If the portsecurity mode was set to "IEEE802.1X Multi-User allow three MAC addresses” and the port Default-VLAN-ID was set to 0, the VLAN-ID send by the RADIUS server was ignored. This has been fixed. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V6.02G]<br>When accessing SNMP Variables of the ifXTable via get-next request, extra invalid OIDs were returned. | ✓ | ✓ | |
| [from V6.02I]<br>Only applies to switches with firmware version V6.01aa or higher:<br>After the update to a newer firmware, which contains new function parameters, these new parameters may contain random values. This has been fixed. | ✓ | ✓ | |
| [from V6.02K]<br>IPv6 access to switch management via SFP ports doesn't work. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02K]<br>If the switch management received a ping request with routing parameters included, the management might hang up. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02K]<br>If both Spanning Tree and CDP were enabled, the "Active Loop Protection" feature for user ports may not work properly. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02K]<br>Only applies to GigaSwitch V5 cable duct switches with PoE+ adapter Rev.B and Rev.B1:<br>Each time the configuration was written to the switch via LANactive Manager, the PoE voltage for the attached PoE end devices was interrupted for a short period. | ✓<br>**HW5** | | |
| [from V6.02L]<br>Only applies to switches with management hardware HW5:<br>If DHCP was enabled and the DHCP server sent an option which contained invalid or useless values for the switch (e.g. option 43 with a value other than the Controller IP address for Zero Touch Configuration), the switch could hang up. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02L]<br>Only applies to switches with management hardware HW5:<br>After resetting a HW5 switch to Factory Default or Factory Default (Except IP Parameters), it was sometimes not possible to access the switch via SSH or SCP. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02L]<br>Only applies to GigaSwitch V5 cable duct switches with Firmware V6.02K:<br>Under certain circumstances the PoE voltage was not enabled, even if a valid PoE end device was connected. Furthermore, the function "Disabled PoE output voltage for a period of 6 seconds" didn't work correctly. | ✓<br>**HW5** | | |
| [from V6.02M]<br>Only applies to switches with management hardware HW5:<br>Activating Multicast parameters "Multicast snooping enable" and "IGMP Querrier enable" in parallel could make the switch unreachable and unusable under certain circumstances. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V6.02M]<br>Only applies to switches with management hardware HW3:<br>IGMP queries sent by HW3 switches were not detected and handled correctly by HW5 switches Multicast features enabled. | ✓<br>**HW3** | ✓<br>**HW3** | |

## 2.6. Release V5.04

## 2.6.1. Release V5.04X

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family HW3➔** | **HW3-Fxx-Pxx-OFFICE** | **HW3-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V5** |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V5** |
| **Manager – Basic Features:** | | | |
| [from V5.03aj]<br>Live Information to show differences between loaded configuration and current device state have been added to tab page 'Device Info' in the Device-Editor. | | | ✓ |
| [from V5.04N]<br>Loading Live Information for current Device-List has been speed up to update the switch status faster. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V5.03aa]<br>Some problems with the GUI on high resolution displays have been fixed. | | | ✓ |
| [from V5.03aa]<br>Wrong time out value for simultaneous firmware update has been fixed. | | | ✓ |
| [from V5.03aa]<br>Client/Controller: In database management view PoE state is now shown as text instead of number. | | | ✓ |
| [from V5.03aa]<br>A bug has been fixed which causes the check column to stay checked after reading the configuration or updating the device successfully. | | | ✓ |
| [from V5.03af]<br>A bug has been fixed which causes an error message when trying to copy a master config to any device from a network drive with read only access. | | | ✓ |
| [from V5.03ai]<br>Client/Controller: During installation of the controller, the database login account is now updated correctly. | | | ✓ |
| [from V5.03ap]<br>Client/Controller: Recovery model of LANactive Manager database has been changed to 'Simple' and the maximum size of the transaction log has been set to 10 GB. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V5.03ak]<br>The per port "LLDP/CDP Neighbor Details" info has been extended with statistic counters for received, transmitted and discarded LLDP and CDP packets. | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| [from V5.03df]<br>Single types of CISCO access points didn't power up to full load via PoE because they request to much power via CDP and LLDP. Now the switch responses with higher power budget to solve this issue. | ✓ | ✓ | |
| [from V5.03du]<br>For the 'Allowed MACs Overflow Address' a new ageing time has been introduced.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Security > Security Setup" the parameter "Portsecurity ageing time for 'Allowed MACs Overflow Address' (minutes)" has been implemented. | ✓ | ✓ | ✓ |
| [from V5.03cv]<br>Only applies to switches with management hardware HW5:<br>Cable diagnostic function for Twisted Pair ports has been implemented. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V5.01eo]<br>Support for the following industrial switch types has been implemented:<br>86 (iGigaSwitch 1004 E+ SFP-4VI HW5)<br>90 (iGigaSwitch 1604 SFP-4VI HW5)<br>91 (iGigaSwitch 1608 SFP-8VI HW5)<br>93 (iGigaSwitch 1612 SFP-12VI HW5) | | ✓ | ✓ |
| [from V5.03ey]<br>Support for new switch types with PoE capability on the uplink port only has been implemented. | ✓ | | |
| [from V5.03ey]<br>Only applies to switches with management hardware HW5:<br>Storage of firmware on memory card has been implemented. If enabled the firmware update takes 10…30 minutes because of the additional memory card write process. During this time the switch is fully functional without any interruption. Only during the final reboot, the switch interrupts all connections for max. 60 seconds.<br>An analog scenario applies if the switches updates itself from the memory card. In this case the switch boots up with the currently installed firmware, loads the config from memory card and starts updating with the firmware from memory card, which is indicated by a blue blinking Mgmt status LED. This update takes also 10…30 minutes, but the switch is fully functional during this time. When the update is finished the switch automatically reboots itself with the new firmware and the Mgmt status LED lights green. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V5.03gh]<br>Showing the size and checksum of Customer-Default / Reboot-Configuration on memory card in NexMan's Device List has been implemented.<br>**Manager – Extensions:**<br>In the Device List the following new columns are displayed by default:<br>"Customer Reboot Config Size", "Customer Reboot Config Checksum", "Customer Default Config Size" and "Customer Default Config Checksum". | ✓ | ✓ | ✓ |
| [from V5.03gh]<br>Showing the Firmware on memory card in NexMan's Device List has been implemented.<br>**Manager – Extensions:**<br>In the Device List the new column "MC Firmware" is displayed by default. | ✓ | ✓ | ✓ |
| [from V5.03gp]<br>The Active Loop Protection function has been enhanced so that loops are also detected if the loop goes through third-party devices (e.g. switches, IP phones). If the loop packet has been received on an uplink port, only the sending user port will be disabled. | ✓ | ✓ | |
| [from V5.03hf]<br>New parameter called "Re-Authentication Inaccessible VLAN mode" implemented. This parameter defines the behaviour of the "Inaccessible VLAN" in case of an IEEE802.1X re-authentication. The IEEE802.1X authentication flow chart has been updated accordingly in the firmware manual.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Security > IEEE802.1X" the parameter "Re-Authentication Inaccessible VLAN mode" has been added. | ✓ | ✓ | ✓ |
| [from V5.04B]<br>Single types of Aruba access points don't power up to full load via PoE because they don't request for power via LLDP. Now the LLDP TLV "IEEE802.3 – Power via MDI" is send by the switch even the end device doesn't request for it. | ✓ | ✓ | |
| [from V5.04C]<br>Only applies to GigaSwitch HW5 cable duct switches with management hardware HW5 and copper uplink with PSE PoE+ adapter:<br>Support for PSE uplink adapter Rev.B has been implemented. This Rev.B uplink adapter may replace Rev.A adapters in future switch deliveries. | ✓<br>**HW5** | | |
| [from V5.04J]<br>VLAN Port Isolation has been extended so that it can be enabled separately per port.<br>Any port for which this function is enabled can communicate exclusively with the uplink ports.<br>Ports that do not have the isolation switched on could communicate with all ports of the Aginode switches in the same VLAN except, of course, with isolated ports.<br>If global VLAN port isolation is disabled, then this feature is disabled for all individual ports. | ✓ | ✓ | |
| [from V5.04G]<br>Support for the following industrial switch type has been implemented:<br>94 (iGigaSwitch 1202 HSR SFP-2VI HW5) | | ✓ | ✓ |
| [from V5.04M]<br>Only applies to iSwitches with management hardware HW5:<br>Support for write-protection of memory card by DIP switch F2 has been implemented. If DIP switch F2 is enabled during reboot, the memory card is write-protected. Any change of F2 while the switch is running has no effect. To indicate that the MC is write-protected, the MC is write-protected, the MC LED lights blue.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Device Info" the parameter "Write-Protection (DIP F2)" has been added. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |
| [from V5.04M]<br>Added reset option to delete firmware on memory card to CLI and WEB.<br>In the CLI the reset command has been extended:<br>`res:et {c:ounter\|b:oots\|o:peration-time\|f:irmware-memory-card}`<br>In the Web Interface, on site "Switch Setup", option "Reset command" has been added.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Management > Agent" Reset Actions "Reset Firmware on Memory Card" and "Total Boots Counter, Reset Port Counters, Total Operation Time, Local Logging and Firmware on Memory Card " have been added. | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| [from V5.04R]<br>If the memory card is removed during runtime and the MAC address from memory card is set as active MAC, the Memory Card LED lights red according to Manager. | ✓ | ✓ | |
| [from V5.04R]<br>Support for the following industrial switch types has been implemented:<br>86 (iGigaSwitch 1004 E+ SFP-4VI HW5)<br>87 (iGigaSwitch 1008 E+ SFP-2VI HW5) | | ✓ | ✓ |
| [from V5.04U]<br>Only applies to industrial switches with high voltage AC/DC power input:<br>Measurement of input voltage has been implemented. Furthermore, it is stated if a AC or DC voltage has been connected to the switch.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "State > Global+Link State" the input voltage will be displayed. | | ✓ | ✓ |
| [from V5.04V]<br>Show alarm in Device List, column "Alarms" of Manager for RADIUS if<br>- a RADIUS server is unreachable<br>- there is a fail in RADIUS or DOT1X authentication on a port.<br>The alarm is automatically cleared if the problem does not persist. | ✓ | ✓ | |
| **Firmware - Security:** | | | |
| [from V5.03ft]<br>A new parameter 'IEEE802.1X Re-authentication initial delay (seconds)' has been implemented. If IEEE 8021.X re-authentication is enabled this time defines the time until the first re-authentication will be initiated. After this first re-authentication the normal 'Re-authentication interval' will be used for further re-authentications.<br>**Manager – Extensions:**<br>In the Device Editor on the 'Security > IEEE 802.1X' tab the parameter 'Re-authentication initial delay (seconds)' has been implemented. | ✓ | ✓ | ✓ |
| **Firmware – SNMP:** | | | |
| [from V5.03du]<br>New SNMP protocol version called " SNMPv3 [Auth.-SHA] [No Priv.] with SNMPv1/SNMPv2c read/only access" implemented. This setting allows read/write access for SNMPv3 without encryption and read/only access for SNMPv1 und SNMPv2c.<br>**Extensions in the Manager:**<br>In the Device-Editor on tab "Management > Access SNMP" the parameter "SNMP Protocol Version" has been extended with the setting "SNMPv3 [Auth.-SHA] [No Priv.] with SNMPv1/SNMPv2c read/only access". | ✓ | ✓ | ✓ |
| [from V5.03fg]<br>Reading the S1 and S2 input voltage for industrial switches via SNMP has been implemented. The new SNMP objects are infoS1InputVoltage and infoS2InputVoltage. | | ✓ | |
| [from V5.03ft]<br>The value of SNMPv3 Engine ID is now manually configurable by the user. If this value is not defined the default MAC based Engine ID will be used.<br>**Manager – Extensions:**<br>In the Device Editor on tab "Management > Access SNMP" the parameter 'Engine ID' has been implemented. | ✓ | ✓ | ✓ |
| [from V5.03gh]<br>Reading the last SNTP time via SNMP has been implemented. The new SNMP object is infoLastSntpTime. | ✓ | ✓ | |
| [from V5.03gh]<br>Reading the size and checksum of Customer-Default / Reboot-Configuration via SNMP has been implemented. The new SNMP objects are infoCfgDefaultSize, infoCfgDefaultChecksum, infoCfgRebootSize and infoCfgRebootChecksum. | ✓ | ✓ | |
| [from V5.03gh]<br>Reading the Firmware on memory card via SNMP has been implemented. The new SNMP object is infoMCFirmware. | ✓ | ✓ | |
| [from V5.03gh]<br>Reading and writing the Alarm Destinations settings via SNMP has been implemented. For this purpose, a new subtree bmSwitchAlarmDest has been added under node bmSwitchMIB, which contains one node bmSwitchAlarmDestSyslogSeverities for the alarm syslog severities of all configurable alarms, and one node bmSwitchAlarmDestTable for the Alarm Destination Table. | ✓ | ✓ | |
| **Firmware – Redundancy:** | | | |
| [from V5.04A]<br>Because the MRP patent has expired, the MRP redundancy feature is available without a AGINODE memory card with MRP license code. Furthermore, MRP has been enabled for Office switches also. | ✓ | ✓ | |
| **Firmware – Bug Fixes:** | | | |
| [from V5.03an]<br>Only applies to switches with management hardware HW5:<br>CDP packets received with a VLAN tag were dropped. This issue has been fixed. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.03cx]<br>If the "Local Logging Mode" was set to "Stop logging on overflow", old log entries were erroneously overwritten. | ✓ | ✓ | |
| [from V5.03es]<br>Only applies to switches with management hardware HW5:<br>When switches were delivered with a pre-configuration, the switch may boot up with fixed IP. After a second reboot the switch starts up with the correct pre-configuration. This issue has been fixed. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.03gw]<br>Only applies to switches with management hardware HW5 and 16 port switches with HW3:<br>Under very rare circumstances the packet transmission from the switch to the end device was interrupted and packets were dropped because of an incompatibility in GigaBit Autonegotiation. This happens normally directly after a power up of the end device. | ✓<br>**HW5** | ✓ | |
| [from V5.03hf]<br>Only applies to switch types iGigaSwitch 541/542<br>The MRP redundancy functionality was not available. This has been enabled for this switch type | | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.03hh]<br>Some IP phones types send different LLDP values for "System Name" during power up which results in two different LLDP entries at the switch. After ageing out the older LLDP entry, the switch sent wrong LLDP-MED values under certain circumstances. This has been fixed. | ✓ | ✓ | |
| [from V5.04C]<br>Only applies to switches with management hardware HW5:<br>If DHCP snooping was enabled, DHCP server packets received on the last uplink port (copper port 6 for 6 port switches, SFP port 7 for 7 port switches, etc.) were dropped under certain circumstances. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.04H]<br>Only applies to switches with management hardware HW5:<br>If an IEEE802.1X end device responded with unicast EAP packets (instead of multicast), authentication failed. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.04J]<br>Only applies to switches with management hardware HW5:<br>VLAN Port Isolation for selected Ports didn't work correctly for management interface und user ports. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.04M]<br>After some days running the switch, in CLI and web the total operation time was set to many years. | ✓ | ✓ | |
| [from V5.04S]<br>The IEEE802.1X supplicant didn't accept EAP multicasts packets if no user port was also set to IEEE802.1X authentication. | ✓ | ✓ | |
| [from V5.04T]<br>Only applies to switches with firmware version V5.04K or higher:<br>Resetting reboot counters via CLI and Manager didn't work correctly. | ✓ | ✓ | |
| [from V5.04U]<br>If the switch didn't get an IP address via DHCP, the log messages were not written to Local Syslog after a suitable time out. | ✓ | ✓ | |
| [from V5.04W]<br>Only applies to switches with management hardware HW5:<br>Under certain circumstances the switch starts from the backup partition after reboot of the switch. Consequently, the switch boots up with the previous installed firmware version. This problem has been fixed. | ✓<br>**HW5** | ✓<br>**HW5** | |
| [from V5.04W]<br>Only applies to iSwitches with management hardware HW3:<br>When the feature was enabled, that the firmware is also stored on memory card, the HW3 Industrial Switches did not close the SCP connection. This problem has been fixed. | | ✓<br>**HW3** | |
| [from V5.04X]<br>Only applies to switches with management hardware HW3:<br>When Accesslist Mode was set to "Enabled for all Access" and no rule was defined, it was not possible to login any more. This problem has been fixed. | ✓<br>**HW3** | ✓<br>**HW3** | |
| [from V5.04X]<br>Only applies to switches with management hardware HW3:<br>In Local Syslog messages for Management Authentication via SSH or SCP the invalid source IP address 0.0.0.0 was indicated. This problem has been fixed. | ✓<br>**HW3** | ✓<br>**HW3** | |

## 2.7. Release V5.02

### 2.7.1. Release V5.02R

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family HW3➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexMan V3** |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **NexMan V5** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Manager – Basic Features:** | | | |
| [from V5.01aa]<br>Support for increased configuration storage area for switches with firmware V5.xx has been implemented. | | | ✓ |
| [from 5.01ag]<br>Scheduled Configuration Download Time was added to "Preferences -> Global". This function allows a time scheduled configuration backup. | | | ✓ |
| [from V5.01as]<br>Support for firmware update of switches with management hardware HW5 has been implemented. Theses firmware images have the file extension ".SWU". | | | ✓ |
| [from V5.01as]<br>The manager now uses PuTTY Secure Copy for file exchange. | | | ✓ |
| [from V5.01.bf]<br>Columns "Power Consumption PoE" and "Input Voltage PoE" have been added to the device list. | | | ✓ |
| [from V5.01.bf]<br>Menu tree in device editor now supports node collapsing. | | | ✓ |
| [from V5.01.bj]<br>MAC Address Table now supports filtering by specific columns. | | | ✓ |
| [from V5.01.bk]<br>The manager now comes with an automatic configurator for the Basic Configuration. The configurator searches for switches in the auto discovery list which have their IP address and user credentials on factory default and configures them either with an IP address taken from a given IP range or with information read from a CSV file. | | | ✓ |
| [from V5.01.bn]<br>Simultaneous download of Config and Local Logging for multiple switches has been added to menu "Configure". Thereby it is possible to read the configuration or local logging from multiple devices at once. | | | ✓ |

| | | | |
|---|---|---|---|
| [from V5.01.bo]<br>The device editor has been changed to a floating window which can be docked to the main grid or used as a single window. In addition, it is possible to open up to four device editors simultaneously to edit and compare multiple devices. | | | ✓ |
| [from V5.02cc]<br>The 'Poll Interval' in the status bar has been replaced by the number of requested devices, showing the progress of the background polling process. | | | ✓ |
| [from V5.01.ck]<br>A progress bar and additional status information for reading and writing multiple devices simultaneously has been added to the status bar. | | | ✓ |
| [from V5.02E]<br>In Client/Controller-Version a user can have a specific number of assigned ports which he is able to see in the device editor and which he can configure. Other ports are not accessible to that user. | | | ✓ |
| [from V5.02E]<br>In preferences on page 'Global' the number of retries for simultaneous reading or writing actions can be set. The specific action will be repeated until it is successful or the maximum number of retries is reached. | | | ✓ |
| [from V5.02E]<br>In preferences on page 'Global' it is now possible to set whether the docking state of the Device-Editor should be saved. Thereby new editors will be created as single window or docked to the main window. | | | ✓ |
| [from V5.02G]<br>A button to lock or unlock the category tree has been added. If the category tree is locked the categories cannot be reordered by dragging them to another position inside the tree. | | | ✓ |
| [from V5.02G]<br>Changed naming of Device-Editor menu items:<br>- Changed text 'Configure' to 'Edit'<br>- Changed text 'Exit & Save' to 'Exit & Save to Database file'<br>- Changed text 'Quit' to 'Cancel' | | | ✓ |
| [from V5.02G]<br>Layer 3 Discovery now comes with simultaneous requests to speed up adding the devices to the device list. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V5.02G]<br>The firmware update process scheduled by Manager started immediately instead of waiting until the given point of time is reached. | | | ✓ |
| [from V5.02G]<br>The Manager crashed when opening the device editor while single firmware update is running. | | | ✓ |
| [from V5.02G]<br>During automatic basic configuration the gateway was not written to the switch. | | | ✓ |
| [from V5.02G]<br>Client/Controller: Manager deleted config-file on startup when application folders are not accessible. | | | ✓ |
| [from V5.02G]<br>Client/Controller: Wrong user credentials led to 'Overtake session' message on log in dialog. | | | ✓ |
| [from V5.02Gf]<br>A bug has been fixed which causes an error when reading the CLI config of any device via the Device-Editor for the first time. | | | ✓ |
| [from V5.02G]<br>A bug has been fixed which causes empty passwords after sending password hashes via master configuration to a switch which has the password encryption mode set to 'standard'. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V5.01aa]<br>The size of the binary configuration storage area has been increased by a factor of three to be ready for any future feature implementations. | ✓ | ✓ | ✓ |
| [from V5.01aa]<br>Ranges support for all CLI commands to configure the PHY interfaces has been implemented.<br>The corresponding CLI commands are:<br>`in:terface {if-no range} ...`<br>Valid values for parameter `{if-no range}` are:<br>`(0...<if-no max>)[-(0...<if-no max>]`<br>Examples:<br>`in:terface 2-5 alarm1 e:nable`<br>`in:terface 1-16 priority-v:lan d:isable`<br>`in:terface 4-8 sp:eed-duplex a:utoneg` | ✓ | ✓ | |
| [from V5.01aa]<br>Ranges support for all CLI commands to configure VLANs (except special VLANs like Default-VLAN or Voice-VLAN) has been implemented.<br>The corresponding CLI commands are:<br>`v:lan-table a:dd {vlan-id range} [<string max. 50 chars>]`<br>`v:lan-table d:elete {vlan-id range}`<br>`v:lan-table pr:io-override {vlan-id range} {d:isable\|(0..7)}`<br>Valid values for `{vlan-id range}` are:<br>`(1...4095)[-(1...4095)]`<br>Examples:<br>`v:lan-table a:dd 1000-1200 VLAN-abc`<br>`v:lan-table d:elete 2-5`<br>`v:lan-table pr:io-override 200-250 d:isable` | ✓ | ✓ | |
| [from V5.01aa]<br>A new VLAN table mode with up to 256 VLANs has been implemented.<br>The corresponding CLI command to enable this mode is:<br>`vlan-table mode 256-static`<br>Hint: Switching from a VLAN table mode with 16 or 64 VLANs to the new mode with 256 VLANs will preserve the existing VLANs in the table. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.01aa]<br>A new port trunking mode called 'hybrid' has been implemented. This mode is only supported if the VLAN table mode has been set to 256 VLANs.<br>The corresponding CLI command to enable this mode is:<br>`interface {if-no range} trunking-mode hybrid`<br>If a port is configured to the hybrid mode an individual per-port membership assignment for each VLAN in the VLAN table can be configured. The membership can be set to "tagged", "untagged" or "not allowed".<br>The corresponding CLI command is:<br>`in:terface {if-no range} vl:an-id {vlan-id range} {t:ag\|u:ntag\|r:emove}` | ✓ | ✓ | ✓ |
| [from V5.01ay]<br>For port security a new RADIUS parameter called 'Cisco device-traffic-class mode' has been implemented. The supported settings are:<br>- Use device-traffic-class=voice to set Voice-VLAN to received VLAN-ID<br>- Use device-traffic-class=voice to allow access to Voice-VLAN | ✓ | ✓ | ✓ |
| [from V5.01az]<br>In the Web interface on webpage “VLAN Table” support for the new VLAN table mode with up to 256 VLANs has been implemented. | ✓ | ✓ | |
| [from V5.01bc]<br>Only applies to industry switches "iSwitch 1604, 1608 and 160C":<br>A per-port bandwidth limiter for received and transmitted packets has been implemented. | | ✓ | |
| [from V5.01bd]<br>The local logging is now activated by factory default for important alarm types. | ✓ | ✓ | |
| [from V5.01cs]<br>A new VLAN Port Isolation Mode 'selected-ports' has been implemented:<br>`v:lan-table po:rt-isolation s:elected-ports`<br>This allows to activate/deactivate the VLAN Port Isolation per port:<br>`in:terface {if-no range} po:rt-vlan-isolation {e:nable\|d:isable}` | ✓ | ✓ | ✓ |
| [from V5.01ea]<br>Support for the following switch types has been implemented:<br>72, 73 and 74 (GigaSwitch V5)<br>75 (GigaSwitch 641 Desk V5)<br>85 (iGigaSwitch 1002 E+ SFP-2VI)<br>93 (iGigaSwitch 1606 HSR SFP-6VI)<br>These switches require separate firmware images with the file extension ".SWU". For updating switches the manager version V5.01bc or higher is required. | ✓ | ✓ | ✓ |
| [from V5.01gp]<br>The display format of the serial number (S/N) has been changed to a unique format: xxxxxNnnnnnn<br>xxxxx = last five digits of the ‘Part Number (P/N)’<br>N = fixed letter<br>nnnnnn = Production number with 6 digits and leading zeros.<br>This applies to the CLI and WEB info pages. In SNMP the unique format is readable via the object infoSeries.<br>Furthermore, the "Production lot" number has been removed because this number was without any relevance.<br>The unique format was already included in the barcode of all delivered switches. From switch generation V5 this unique serial number is also printed below the barcode and marked with ‘S/N’.<br>**Manager – Extensions in V5.01au:**<br>In the Device Editor on tab ‘Device Info’ the format of ‘Serial number’ has been changed accordingly.<br>In the Device-List the name of column ‘Serie/No’ has been changed to ‘Serial Number (S/N)’. To show the new format in this column the switches must be updated with the firmware V5.01gp or higher.<br>In the Excel and XML Inventory-List the format of the column ‘Device - Serial Number (S/N)’ has been changed accordingly<br>The "Production lot" number has been removed from all info pages and lists. | ✓ | ✓ | ✓ |
| [from V5.01gj]<br>Only applies to switches with management hardware HW5:<br>The ping response times have been optimized so that the average response time is about 1 ms. | ✓ | ✓ | |
| [from V5.01ia]<br>The following LLDP-MED extensions for location identification have been implemented:<br>[25] building (structure)<br>[26] unit (apartment, suite)<br>[29] type of place/ placetype | ✓ | ✓ | ✓ |
| [from V5.01kg]<br>The extended local Admin-1 account has been extended with a new configuration setting called “Admin-1 Access rights”. The available options are:<br>- Read/Write for all parameters (factory default)<br>- Read/Only for all parameters except Port Monitor on WEB<br>**Manager - Extensions:**<br>In the Device Editor on tab “Management > Local Accounts” in group “Extended Admin Account Setup (Read/Write)” the parameter “Admin-1 Access Rights” has been added. | ✓ | ✓ | ✓ |
| [from V5.01kx]<br>The source MAC address of all LLDP and CDP packets has been changed to active MAC address of the switch. Previously each port used a different so called “Port MAC Address”. | ✓ | ✓ | |
| [from V5.01ma]<br>Support for the following switch type has been implemented:<br>76 (GigaSwitch 642 Desk V5)<br>These switch require separate firmware images with the file extension ".SWU". For updating switches the manager version V5.01bc or higher is required. | ✓ | ✓ | ✓ |
| [from V5.01mm]<br>The time client has been extended with a second “Time server IP 2” address. If this second address is configured the switch requests the time from both configured servers simultaneously.<br>**Manager - Extensions:**<br>In the Device Editor on tab “Time Client > SNTP Setup” the parameter “Time Server IP 2” has been added. | ✓ | ✓ | ✓ |
| [from V5.01mq]<br>Only applies to industrial switches "iSwitch 54x, 74x and 104x"":<br>Support for management hardware version 3.05 implemented. | | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.01mr]<br>Support for Extreme (ex Avaya) Fabric Attach has been implemented. Per VLAN table entry a SPBM I-SID can be configured. The FA authentication key is “Aginode” by default but can be re-configured to a customer defined value if need. Note: This feature requires that LLDP is enabled.<br>**Manager - Extensions:**<br>In the Device Editor on tab “VLAN Setup” the parameters “Fabric Attach Authentication Key” and “SPBM I-SID” have been added. | ✓ | ✓ | ✓ |
| [from V5.01ms]<br>By factory default LLDP is now enabled and CDP is disabled. LLDP has become the widely used standard discovery protocol and should be used in any environment if possible. | ✓ | ✓ | |
| [from V5.01ms]<br>By factory default LLDP is now enabled and CDP is disabled. LLDP has become the widely used standard discovery protocol and should be used in any environment if possible. | ✓ | ✓ | |
| [from V5.01of]<br>The line editing features for CLI have been extended with all standard editing functions (moving back and forward within a line, inserting and deleting text within a line, jump to start an end of a line, etc.) extended. Furthermore pasting many command lines into CLI has been improved. | ✓ | ✓ | |
| [from V5.01qf]<br>A new CDP-Mode called “Enabled with entry in LLDP-MIB“ has been implemented. By enabling this mode CDP neighbor entries are readable via the SNMP LLDP-MIB. | ✓ | ✓ | ✓ |
| [from V5.01qf]<br>A new LLDP-Mode called “Disabled with LLDP filter“ has been implemented. This mode filters all LLDP packets received from attached end devices or core switches. The already existing mode “Disabled” has been renamed to “Disabled without LLDP filter” because this mode forwards all received LLDP packets to all ports assigned to the same VLAN-ID. | ✓ | ✓ | ✓ |
| [from V5.01qf]<br>A new CDP-Mode called “Disabled with CDP filter“ has been implemented. This mode filters all CDP packets received from attached end devices or core switches. The already existing mode “Disabled” has been renamed to “Disabled without CDP filter” because this mode forwards all received CDP packets to all ports assigned to the same VLAN-ID. | ✓ | ✓ | ✓ |
| [from V5.01ra]<br>The allowed characters for all names and passwords have been extended and unified.<br>Allowed are now:<br>**a-z A-Z 0-9 . , ; ! " ' % # $ & ^ ~ @ * : + - = _ / \ \| ( ) [ ] { } < >**<br>These characters are allowed and checked in WEB, CLI and Manager input masks.<br>The only exceptions are the following not supported characters:<br>**?** (ASCII 63) Can't be used because in CLI console “?” is always interpreted as help command<br>` (ASCII 96) User must press keys <shift + `> + <space> to enter this character, which is not useful | ✓ | ✓ | ✓ |
| [from V5.01re]<br>Support for the following switch type has been implemented:<br>77 (GigaSwitch V3 with management hardware version 3.50) | ✓ | ✓ | ✓ |
| [from V5.01re]<br>Only applies to industrial switches with alarm output contacts and function inputs:<br>Clearing active alarm outputs via function inputs has been implemented.<br>The following two options are available for each function input:<br>- Clear all active Output Alarm when Function Input opened<br>- Clear all active Output Alarm when Function Input shorted<br>**Manager - Extensions:**<br>In the Device Editor on tab “Alarms > Alarm Inputs” the parameter “Function Input x Alarm Mode” has been extended with the above options. | | ✓ | ✓ |
| [from V5.01rr]<br>Does only apply to the 16 port industrial switches:<br>The IEC61850 model has been extended so that the current alarm state of the two outputs contacts are readable via the new objects GGIO1.SPCCO1 and GGIO1.SPCCO2. | | ✓ | ✓ |
| [from V5.02C]<br>To prevent network loops in Spanning Tree topologies, the internal timeouts for missing received BPDUs has been modified. This makes the topology much more stable in case that the Aginode switch is not the root bridge of the particular Spanning Tree domain. | ✓ | ✓ | |
| [from V5.02D]<br>Only applies to GigaSwitch V5 cable duct switches with management hardware HW5 and PoE+ functionality for the four front copper ports:<br>Support for PoE+ adapter Rev.B has been implemented. This Rev.B head adapter may replace Rev.A adapters in future switch deliveries. | ✓ | | |
| [from V5.02D]<br>Support for switch type “GigaSwitch V5 TP(PD-F+) SFP-VI 48/54VDC” has been implemented. This switch type supports forwarding of PoE power from the copper uplink port to the four front site copper ports with up to 25 Watts. | ✓ | | |
| [from V5.02F]<br>Only applies to switches with management hardware HW5:<br>Time for deleting log logging messages has been significantly reduced. | ✓ | ✓ | |
| [from V5.02H]<br>Does only apply to industrial switches:<br>The IEC61850 model has been extended so that the current alarm states of the two outputs contacts are readable via the standard objects GGIO1.SPCSO1 and GGIO1.SPCSO2. Depending on the “Alarm Output M1/M2 Mode” the ctlModel is switched between 0 (status-only) and 1 (direct-with-normal-security). | | ✓ | |
| [from V5.02I]<br>Only applies to switches with management hardware HW5:<br>The IEEE802.1p “VLAN based Priority Override” feature has been implemented. | ✓ | ✓ | |
| **Firmware - Security:** | | | |
| [from V5.01ky]<br>For SSH/SCP the unsecure Hash algorithm SHA1 has been removed. As a result, only the secure SHA2 based algorithm are supported (SHA-256 and SHA-512). | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.01pc]<br>Configuration of the minimum allowed TLS version for HTTPS access implemented. The available settings are:<br>• Allow TLS 1.0 and higher<br>• Allow TLS 1.1 and higher<br>• Allow TLS 1.2 and higher<br>**Manager - Extensions:**<br>In the Device Editor on tab 'Access Global' the parameter "Allowed TLS versions" has been added. | ✓ | ✓ | ✓ |
| [from V5.01qk]<br>Only applies to switches with management hardware HW3:<br>The WEB browser Chrome 65 or higher reported a security issue called ERR_SSL_VERSION_INTERFERENCE.<br>Furthermore, the WEB browser Firefox Qunatum 60 or higher reported a security issue called SSL_ERROR_NO_RENEGOTIATION_ALERT.<br>The HTTPS server has been extended to allow access now. | ✓ | ✓ | |
| [from V5.01qr]<br>Ports, which were disabled via DHCP snooping, can now optionally be re-enabled automatically after a settable time value. The time value can be set in the range from 1 to 60000 seconds.<br>**Manager - Extensions:**<br>In the Device Editor the 'Re-Enable Time for DHCP-Snooping-Disabled ports' parameter has been implemented on the 'DHCP Relay / Snooping' tab. | ✓ | ✓ | ✓ |
| [from V5.01nh]<br>Implementing SSH and SCP access according to the BSI (Bundesamt für Sicherheit in der Informationstechnik) recommendation "Technische Richtlinie TR-02102-4":<br>Added key exchange method:<br>• ecdh-sha2-nistp256<br>Added server key algorithms:<br>• ecdsa-sha2-nistp256<br>Added Hash Methods:<br>• hmac-sha2-256<br>• hmac-sha2-512<br>Furthermore the new elliptic curve method and algorithms allows much faster SSH and SCP access if the client also supports it. | ✓ | ✓ | |
| [from V5.01sa]<br>Only applies to switches with management hardware HW5:<br>The HTTPS server certificate has been extended from 1024 to 2048 bit. (RSA, 2048 Bit Key, SHA-256). | ✓ | ✓ | |
| [from V5.01sy]<br>Positive and negative user authentications for NexMan, WEB and CLI are now logged with interface, user name, IP address, status (success or failure) and access rights (Read/Write or Read/Only).<br>Furthermore each configuration change is logged with interface, user name and IP address. | ✓ | ✓ | |
| [from V5.02B]<br>Only applies to switches with management hardware HW3:<br>The HTTPS server has been hardened to withstand the ROBOT attack according to BSI (Bundesamt für Sicherheit in der Informationstechnik) report "CSW-Nr. 2017-244792-10k3". | ✓ | ✓ | |
| **Firmware – Redundancy:** | | | |
| [from V5.01hf]<br>Only applies to industrial switches with 16 ports and to all switches with management hardware HW5:<br>Multiple Spanning Tree (MSTP) has been implemented. | ✓ | ✓ | |
| [from V5.01hz]<br>Only applies to industrial switches with 16 ports and to all switches with management hardware HW5:<br>Link Layer Aggregation (LACP) has been implemented. | ✓ | ✓ | |
| **Firmware – SNMP:** | | | |
| [from V5.01kz]<br>Setting VLAN prioritization override for IEEE802.1p has been added to the Private MIB.<br>The corresponding SNMP OIDs in MIB version V5.01kz are portPrioOverride and vlanPrioOverride. | ✓ | ✓ | |
| [from V5.02A]<br>The file name of the Private MIBs have been renamed to be compliant with most MIB compiles.<br>The new names are:<br>• AGINODE-MIB.mib - Global MIB for all Aginode products<br>• AGINODE-BM-MIB.mib - product-specific MIB for Aginode office and industrial switches | ✓ | ✓ | |
| [from V5.02B]<br>The filenames of the Private MIBs have been renamed to be compliant with most MIB compilers:<br>• AGINODE-MIB.mib - Global MIB for all Aginode products<br>• AGINODE-BM-MIB.mib - product-specific MIB for Aginode office and industrial switches | ✓ | ✓ | |
| [from V5.02B]<br>Change name and content of the following SNMP traps:<br>- trap switchMgmtAuthFailure renamed to switchMgmtAuth<br>- trap radiusMgmtAuthReject renamed to radiusMgmtAuth<br>- trap switchConfigurationChanged<br>The SNMP Private MIBs have been updated to version V5.02B. | ✓ | ✓ | |
| **Firmware – Bug Fixes:** | | | |
| [from V5.01bc]<br>Only applies to switches with firmware V4.13ba or higher:<br>When using Multiple Spanning Tree, MST Internal ports were detected incorrectly as Boundary ports under certain circumstances. | ✓ | ✓ | |
| [from V5.01bc]<br>Only applies to industry switches "iSwitch 1604, 1608 and 160C":<br>If the VLAN trunking mode of a port was configured to Disabled, Tagged packets of invalid VLANs are received and forwarded under certain circumstances. | | ✓ | |
| [from V5.01bt]<br>The LLDP Protocol now includes the PoE power values for "Allocated Power" via IEEE 802.3 Organizationally Specific TLV "Power-Via-MDI" and LLDP-MED TLV "Extended Power-Via-MDI". | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.01dh]<br>The requested power values from a PoE device via CDP were not transmitted properly. As a result, the PoE device could not boot completely. | ✓ | ✓ | |
| [from V5.01dk]<br>The read and write of the configuration via CLI get/put command was not working. | ✓ | ✓ | |
| [from V5.01dm]<br>It was not possible to edit the MGMT VLAN ID via web interface. | ✓ | ✓ | |
| [from V5.01dm]<br>Reading the der Alarm Outputs M1 and M2 always returned the value (1) notSupported | ✓ | ✓ | |
| [from V5.01fb]<br>In some cases, the LLDP transmitted wrong PoE power values to connected IP-Phones. Especially when several IP-Phones were connected to the same switch. This causes the IP-Phones to reboot. | ✓ | ✓ | |
| [from V5.01fb]<br>While accessing the SNMP Variable lldpRemManAddrOID via get request sometimes wrong OIDs returned. This happened especially when several LLDP devices were connected to the same switch. | ✓ | ✓ | |
| [from V5.01ft]<br>Only applies to switches with management hardware HW5:<br>The numbering of the two SFP uplink ports for switch type “GigaSwitch V5 SFP-2VI” was crossed compared to the equivalent V3 switches. The two SFP slot are therefore logically crossed in V5 so that the numbering is identical to V3 switches. Port 5 is left (power connector side) and Port 6 is right (function input connector side). | ✓ | | |
| [from V5.01fv]<br>Only applies to switches with management hardware HW5:<br>IP packets send by the switch, had the "Don't fragment" flag set. Under certain circumstances this flag causes problems in router or firewall environments. This flag is cleared now. | ✓ | ✓ | |
| [from V5.01ga]<br>In WEB interface on page “Port State” the column “Active Default VLAN-ID” shows the wrong status text. | ✓ | ✓ | |
| [from V5.01gg]<br>Only applies to switches with management hardware HW5 and enabled RSTP function:<br>The topology was not calculated correctly under certain circumstances. It is strongly recommended to update to this version if Spanning Tree is used. | ✓ | ✓ | |
| [from V5.01gy]<br>Only applies to switches with management hardware HW5 and enabled DHCP client:<br>After changing the VLAN of the management port the new DHCP request doesn’t correctly send an empty “Client-IP” field inside the request packet. | ✓ | ✓ | |
| [from V5.01ic]<br>RADIUS Accounting sends wrong values under certain circumstances. | ✓ | ✓ | |
| [from V5.01hm]<br>Only applies to switches with management hardware HW5:<br>After an undefined runtime of the switch, the internal time calculation delivered wrong values. Thus, all time-based functions (e.g. DHCP) worked incorrect. Furthermore, all displayed time values (e.g. Uptime, Time since last link change) were wrong with values of 10.000 days or higher. | ✓ | ✓ | |
| [from V5.01hz]<br>Only applies to switches with management hardware HW5:<br>Enabling IPv4 access list entries causes interruption of IPv4 access. | ✓ | ✓ | |
| [from V5.01ks]<br>Only applies to switches with management hardware HW5:<br>CDP packet were not displayed in neighbor table if the default VLAN of the receiving port was not the management VLAN. | ✓ | ✓ | |
| [from V5.01ks]<br>Only applies to switches with management hardware HW5:<br>Changing the port default VLAN via RADIUS server causes a short interruption of other ports under certain circumstances | ✓ | ✓ | |
| [from V5.01kt]<br>Only applies to switches with management hardware HW5:<br>If function “Encrypt passwords in CLI” was enabled the shown encrypted strings were not compatible with switches with management hardware HW3. Now the encrypted strings are identical for HW3 and HW5 switches. | ✓ | ✓ | |
| [from V5.01kt]<br>Only applies to switches with firmware V5.01ed or higher:<br>The CLI command “radius accounting …” was not accepted. | ✓ | ✓ | |
| [from V5.01kx]<br>Only applies to switches with management hardware HW5:<br>The port Speed/Duplex setup “ECO 10/100” was not handled correctly for TP ports and SFP ports with a Copper SFP inserted. Furthermore, if a Copper SFP was admin disabled and re-enabled, the link speed was wrong under certain circumstances. | ✓ | ✓ | |
| [from V5.01ma]<br>Under certain circumstances some details of CDP neighbors were not shown correctly in the neighbors table. | ✓ | ✓ | |
| [from V5.01ma]<br>The CLI commands “tftp check-min-fw <version-number> …” and “tftp check-this-fw <version-number> …” doesn't worked correctly if a <version-number> with one or two subversion letters were given as parameter, e.g. 414W or 413aa. The sub version letters were ignored and so an automatic upgrade or downgrade was only possible if the main version number was different. Now the sub version letters are significant also. | ✓ | ✓ | |
| [from V5.01mf]<br>Only applies to switches with management hardware HW5:<br>Port statistic counters were not correctly displayed in WEB interface. | ✓ | ✓ | |
| [from V5.01mk]<br>Only applies to switches with management hardware HW5:<br>Accessing the LLDP Remote Address Table via SNMP (lldpRemManAddrTable) results in wrong IP addresses inside the SNMP response packets. | ✓ | ✓ | |
| [from V5.01mk]<br>Accessing the new unique serial number via SNMP OID infoSerie results in some extra characters at the end of the serial number. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.01mp]<br>Only applies to switches with firmware V5.01gb or higher:<br>Reading SFP info and diagnostic values via SNMP results in wrongly formatted SNMP response packets. | ✓ | ✓ | |
| [from V5.01mr]<br>Only applies to switches with management hardware HW3 with cable test functionality:<br>Starting the cable test via WEB interface for a port 2 or higher, wrongly measures port 1. | ✓ | ✓ | |
| [from V5.01mx]<br>RADIUS re-authentication of the same MAC doesn't work correctly if the first authentication sets a port Default VLAN and the second one sets no VLAN. After the second authentication, the VLAN of the first authentication wrongly stays valid | ✓ | ✓ | |
| [from V5.01nh]<br>Only applies to switches with management hardware HW5:<br>The time scheduled firmware update via time server doesn't works correctly. | ✓ | ✓ | |
| [from V5.01oc]<br>Only applies to office switches with management hardware HW3 and firmware V5.01hk or higher:<br>Attached PoE Class 4 end devices were not powered correctly under certain circumstances. | ✓ | | |
| [from V5.01og]<br>SNMP get-requests to SNMP MIB tree 'dot1qTpFdbTable' of Q-BRIDGE-MIB always results in error message "noSuchName". | ✓ | ✓ | |
| [from V5.01ow]<br>Accessing an empty LLDP MIB tree via SNMPv2/v3 get-request now correctly return "no such instance" instead of "no such object". | ✓ | ✓ | |
| [from V5.01pe]<br>Only applies to switches with management hardware HW5:<br>After an uptime of "49 days : 17 hours : 2min" the uptime was reset and starts counting up from zero. If a reset occurs, it results in high values for "Time since last link change" and wrong SNTP date values. Furthermore, other time based functions maybe effected.<br>We strongly recommend to update to this firmware version or a higher version. | ✓ | ✓ | |
| [from V5.01pg]<br>Only applies to switches with function input contacts:<br>If the function input alarm mode was set to a mode without "CLEAR" the switch wrongly sends clear packets if the alarm was not active. | ✓ | ✓ | |
| [from V5.01pk]<br>Only applies to switches with management hardware HW5:<br>If a memory card was inserted the switch management access was blocked for up to 15 seconds if the configuration of the switch was changed. | ✓ | ✓ | |
| [from V5.01qt]<br>Only applies to switches with management hardware HW5:<br>If the IP address setup of the switch was configured to get the IP address via DCHP, under certain circumstances the switch reboots after approximately 1000 DHCP lease time outs. With standard lease times of many days this issue is not critical because a reboot may happen after many years. | ✓ | ✓ | |
| [from V5.01qk]<br>Only applies to switches with management hardware HW5:<br>Under certain circumstances the switch doesn't accepts a correct firmware via LANactive Manager or SCP. This problem has been fixed.<br>Hint: To update a switch with this problem try to reboot switch and repeat update. If this doesn't solve the problem please reset the switch to factory and retry. | ✓ | ✓ | |
| [from V5.01qx]<br>Only applies to switches with management hardware HW5:<br>The reboot reason inside cold start alarms was wrong under certain circumstances. | ✓ | ✓ | |
| [from V5.01sr]<br>Only applies to switches with management hardware HW5:<br>Under certain circumstances IGMP query packets were not forwarded to untagged user ports if IGMP Snooping was enabled. | ✓ | ✓ | |
| [from V5.02B]<br>If the Manager authentication was set to UDP/TFTP with RADIUS authentication, passwords longer than 14 characters were not accepted. | ✓ | ✓ | ✓ |
| [from V5.02B]<br>Only applies to switches with management hardware HW5:<br>CDP neighbors which send VLAN-tagged CDP packets were not displayed in the LLDP/CDP Neighbors table. | ✓ | ✓ | |
| [from V5.02B]<br>Spanning Tree debug messages written to the local log were truncated after the first letter. Furthermore alarm messages which include a MAC address were written or send with a truncated MAC address. | ✓ | ✓ | |
| [from V5.02C]<br>Only applies to switches with management hardware HW5:<br>If a time scheduled firmware update was executed via Manager or SCP, and the switch had no valid time received from a time server, the update was rejected by the switch without any notice to the user. Now the user will get a corresponding error message. | ✓ | ✓ | |
| [from V5.02D]<br>The SNMPv3 Engine ID printed in the CLI configuration (e.g. in command 'show running-config') was partly wrong. Some '0' values were not printed. This was only a cosmetically issue because the Engine ID was used correctly within the SNMPv3 protocol itself. | ✓ | ✓ | |
| [from V5.02E]<br>Only applies to switches with management hardware HW3:<br>Firmware update has been stabilized in case of interruption in SCP firmware file transfer. | ✓ | ✓ | |
| [from V5.02G]<br>Only applies to switches with management hardware HW3:<br>The number of alarm messages in case of internal management warnings has been limited to prevent an overflow of the local log file. | ✓ | ✓ | |
| [from V5.02H]<br>Only applies to switches with firmware version V5.01kx or higher:<br>Switches were not protected against a downgrade to a firmware version which was below the minimum required version. Please update those switches to firmware version V5.02H to prevent a not suitable downgrade. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V5.02I]<br>If Spanning Tree debugging to local log was enabled, link up and down debug messages were logged even Spanning Tree was disabled for the particular port. | ✓ | ✓ | |
| [from V5.02J]<br>The IEEE802.1p "VLAN based Priority Override" didn't work for the first VLAN-ID configured in the VLAN-Table. | ✓ | ✓ | |
| [from V5.02K]<br>Only applies to switches with management hardware HW5:<br>If DHCP snooping was enabled for a particular port, received IP packets with a 'Fragmentation Offset' greater than 0 were dropped. | ✓ | ✓ | |
| [from V5.02K]<br>Ping from Switch to other devices didn't work via CLI or Manager under certain circumstances. | ✓ | ✓ | ✓ |
| [from V5.02M]<br>Only applies to switches of type GigaSwitch V3 with SC or ST fiber optic interfaces and with firmware version V5.01gf or higher:<br>The TX power of the fiber optic SC or ST transceiver module was permanently disabled | ✓ | | |
| [from V5.02M]<br>Only applies to switches with management hardware HW5:<br>If Spanning Tree was enabled IGMP control packets were wrongly forwarded through blocked ports under some circumstances. | ✓ | ✓ | |
| [from V5.02N]<br>Only applies to switches with management hardware HW5:<br>SNMP get requests to the LLDP-MIB for the objects lldpLocSysCapSupported, lldpLocSysCapEnabled, lldpRemSysCapSupported and lldpRemSysCapEnabled returned wrong values. | ✓ | ✓ | |
| [from V5.02P]<br>Only applies to switches with management hardware HW5:<br>Under certain circumstances a firmware update failed and had to be restarted. | ✓ | ✓ | |
| [from V5.02P]<br>Only applies to switches with management hardware HW5:<br>For switches with part number 88303953 the switch hardware version was wrongly reported with version 5 instead of 2 under certain circumstances. | ✓ | ✓ | |
| [from V5.02Q]<br>Only applies to switches with management hardware HW5:<br>For switches with part number 88303953 the switch hardware version was wrongly reported with version 5 instead of 2 under certain circumstances. | ✓ | ✓ | |
| [from V5.02Q]<br>The DHCP snooping re-enable time was wrongly displayed and configured via the switch manager software. Configuring via CLI was correct. Please use firmware V5.02Q or above together with Manager V5.02F or above for correct configuration of the DHCP snooping re-enable time. | ✓ | ✓ | ✓ |
| [from V5.02R]<br>If the portsecurity mode was set to IEEE802.1X with MAC bypass and the MAC address was learned via the first EAP packet, the immediate MAC bypass didn't work correctly. | ✓ | ✓ | |
| [from V5.02R]<br>If the spanning tree debugging mode was enabled, the debugging messages were also send to an eventually configured SYSLOG server instead of sending to local SYSLOG only. | ✓ | ✓ | |

## 2.8. Release V4.14

### 2.8.1. Release V4.14X

| **Switch family ➔** | **Office** | **Industrie** | **Manager** |
|---|---|---|---|
| **Firmware family ➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Redundancy:** | | | |
| [from V4.14X]<br>To prevent network loops in Spanning Tree topologies, the internal timeouts for missing received BPDUs has been modified. This makes the topology much more stable in case that the Aginode switch is not the root bridge of the particular Spanning Tree domain. | ✓ | ✓ | |

### 2.8.2. Release V4.14W

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family ➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.14W]<br>In WEB interface on page "Port State" the column "Active Default VLAN-ID" shows the wrong status text. | ✓ | ✓ | |

### 2.8.3. Release V4.14V

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|

| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
|---|---|---|---|
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.14V]<br>Setting the VLAN Table Mode via SNMP doesn't works under certain circumstances. | ✓ | ✓ | |

## 2.8.4. Release V4.14U

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.14U]<br>Only applies to switches with firmware V4.13ba or higher:<br>When using Multiple Spanning Tree, MST Internal Ports were detected incorrectly as a Boundary Port under certain circumstances. | ✓ | ✓ | |
| [from V4.14U]<br>Only applies to industry switches "iSwitch 1604, 1608 and 160C":<br>If the VLAN trunking mode of a port was configured to Disabled, Tagged packets of invalid VLANs are received and forwarded under certain circumstances. | | ✓ | |

## 2.8.5. Release V4.14T

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware – Basic Features:** | | | |
| [from V4.14T]<br>The LLDP protocol sends now the PoE power values via IEEE 802.3 Organizationally Specific TLV "Power-Via-MDI" and LLDP-MED TLV "Extended Power-Via-MDI". | ✓ | ✓ | |
| [from V4.14T]<br>RADIUS requests now contain the attribute "Tunnel-Private-Group-ID". This attribute is for diagnostic purposes only and must be ignored by the RADIUS. It contains the VLAN ID of the MAC address of the end device to be authenticated, the authentication status of the end device, and the current port default and voice VLAN IDs of the switch port. | ✓ | ✓ | |
| **Firmware - Bugfixes:** | | | |
| [from V4.14T]<br>Problem while applying customer pre-configuration in factory resolved. | ✓ | ✓ | |
| [from V4.14T]<br>Under certain time-critical packet sequences, the port default VLAN assigned via RADIUS Server could be overridden if the telephone and PC were simultaneously authenticated via IEEE802.1X. | ✓ | ✓ | |
| [from V4.14T]<br>If the IP address of the switch was changed by the DHCP server in response to a DHCP-Request/DHCP-Acknowledge sequence (without DHCP Discover), this new IP address was not shown in manager and SNMP Requests. | ✓ | ✓ | |

## 2.8.6. Release V4.14R

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.14R]<br>Applies only to „GigaSwitch 541/542 Desk“ switches:<br>After reboot the red Set-LED at the front site of the switch lights permanently. | ✓ | | |
| [from V4.14R]<br>The LLDP attribute "OID String" included in the TLV "Management Address" was not completely implemented in LLDP and thus not accessible via the SNMP LLDP-MIB. | ✓ | ✓ | |
| [from V4.14R]<br>Accessing the SNMP MIB trees dot1dStp, lldpConfiguration and lldpLocalSystemData via SNMP Get-Request returns partly wrong OIDs. | ✓ | ✓ | |

## 2.8.7. Release V4.14Q

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|

| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
|---|---|---|---|
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.14Q]<br>The LED Mode "Show Link" for the green port LEDs was not completely implemented in CLI, WEB and SNMP. New SNMP MIB version is V4.14Q. | ✓ | ✓ | |
| [from V4.14Q]<br>The textual description for internal voltages and temperature in CLI command "show info" were missed. | ✓ | ✓ | |

## 2.8.8. Release V4.14P

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Manager – Basic Features:** | | | |
| [From V4.10ao]<br>The SNMPv3 Manager access mode was removed. | | | ✓ |
| [From 4.10ak]<br>The Templates menu options have been extended by the "Copy Configuration Templates to checked Devices" option. This feature allows you to distribute configuration files to up to 100 devices simultaneously. The configuration files include: Master-Configuration, Customer Reboot Configuration, Customer Default Configuration and Running Configuration. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [From V4.10ao]<br>If for a port name more than 15 characters were entered, the 16th character was discarded when writing the configuration. | | | ✓ |
| [From V4.10ab]<br>New devices detected via Layer-3 Autodiscover were not added to the Device-List. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [From V4.14K]<br>After booting switches of the iSwitch 1604, 1608, and 160C types the SFP ports are now added with a certain delay, in order to reliably prevent loops in ring topologies. If a ring topology is used with the MSTP, RSTP or MRP redundancy protocols, we urgently recommend using an SFP port for at least one of the two ring ports. | | ✓ | |
| [From V4.14G]<br>Does only apply to Office Switches of the GigaSwitch V3 and GigaSwitch Desk types:<br>The UPLINK-TP, if any, was set to Uplink/Downlink in the Default Configuration. This prevents the link from being disabled unintentionally when DHCP snooping is activated. Now the following ports are set to Uplink/Downlink in the Default Configuration:<br>- All rear ports on the cable duct switch.<br>- All ports with fixed optics, such as ST and SC.<br>- All SFP ports. | ✓ | | |
| [From V4.14G]<br>Now the "MAC Address Table per Port" can be indicated in the CLI. | ✓ | ✓ | |
| [From V4.14C]<br>When editing the local accounts, passwords containing invalid characters are rejected. However, this will only work, if the password is entered in plain text and not as a hash. | ✓ | ✓ | |
| [From V4.14C]<br>Now it is possible to administratively disable an Uplink/Downlink port.<br>**Manager – Extensions:**<br>The Admin State of an Uplink/Downlink port was extended by the Disabled option. | ✓ | ✓ | ✓ |
| [From V4.13bn]<br>The configurations „Customer Default Config" and „Customer Reboot Config" were added.<br>This feature is not supported by Management hardware versions 3.01, 3.02, 3.03 and 3.10. | ✓ | ✓ | |
| [From V4.13ba]<br>The IEEE802.1p "VLAN based Priority Override" feature has been implemented. It allows the IEEE802.1p Priorityvalue to be overwritten depending on the VLAN-ID of the received packet.<br>**Manager – Extensions:**<br>In the Device Editor the "IEEE802.1p VLAN based priority override enable" option has been added to the Port tab. Moreover, there is a new column in the VLAN Table for configuring the 802.1p based priority override value on the VLAN Table tab. | ✓ | ✓ | ✓ |
| [From V4.13af]<br>Five additional Admin accounts have been added. All these accounts have the same authorization level.<br>**Manager – Extensions:**<br>In the Device-Editor the Admin accounts Admin-1 to Admin-5 have been added to the Local Accounts tab. | ✓ | ✓ | ✓ |
| [From V4.13af]<br>The Configuration Change Info trap has been extended by the account name. | ✓ | ✓ | |
| [From V4.13ad]<br>802.1x transparency has also been implemented for those ports whose security mode is set to "IEEE802.1x Supplicant with MD5 Challenge". This provides the advantage that both the switch and the connected terminal devices can be authenticated via the core switch. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [From V4.13aa]<br>From firmware version V4.13aa the following switch types are no longer supported:<br>Type Designation<br>50 GigaSwitch BM+<br>51 GigaSwitch BM+<br>52 GigaSwitch V2+<br>53 GigaSwitch V2+<br>54 GigaSwitch V2+<br>55 GigaSwitch V2+<br>56 GigaSwitch V2+<br>V4.12C is the last available firmware for these switch types. In future, only bug fixes will be performed for this firmware.<br>**CAUTION: Firmware version V4.13aa or later must NOT be installed on these switch types. Otherwise the switch will not boot correctly.** | ✓ | | |
| [From V4.11dt]<br>Even if no Voice VLAN is configured for the respective port, now the LLDP-MED Network-Policies (Application Type Voice and Application Type Voice Signaling) will be sent. | ✓ | ✓ | |
| [From V4.11dn]<br>Now the cause for rebooting a device is added in the Local Syslog and in the Remote Syslog. | ✓ | ✓ | |
| [From V4.11ad]<br>For SFP ports configured to Admin Disabled, now principally no SFP alarms will be sent. | ✓ | ✓ | |
| [From V4.11ao]<br>Does only apply to industrial switches:<br>Now the Memory Card Mode allows you to disable the memory card feature. Previously this feature was only supported for office switches. The following options are available:<br>• Enabled<br>• Disabled<br>• Permanently Disabled<br>Manager – Extensions:<br>In the Device Editor the “Memory Card Mode” parameter has been implemented on the “Agent” tab. | ✓ | ✓ | ✓ |
| [From V4.11aq]<br>If authentication for SSH, SCP, TELNET or V.24 is made via a RADIUS server, now the names and passwords up to a length of 64 characters will be accepted. Previously the length was limited to 14 characters. | ✓ | ✓ | |
| **Firmware - Security:** | | | |
| [From V4.14D]<br>For the “Portsecurity - Failure Action” a new mode called “Disable Port immediately after wrong MAC or Authentication” has been implemented. This means that the respective port will be disabled, if authentication was refused by the RADIUS Server in the 'RADIUS …' and 'IEEE802.1X …' security modes.<br>**Manager – Extensions:**<br>The Security Failure Action on the Security Setup tab has been extended by the “Disable Port immediately after wrong MAC or Authentication” item. | ✓ | ✓ | ✓ |
| [From V4.14K]<br>For the local Login account the SHA256 Hash Password Encryption Mode has been added.<br>**Manager – Extensions:**<br>In the Device Editor the Password Encryption Mode has been extended by the SHA256 Hash setting on the Local Accounts tab. | ✓ | ✓ | ✓ |
| [From 4.13be]<br>For HTTPS access some WEB browsers, such as Google Chrome, showed the following error message: ERR_SSL_FALLBACK_BEYOND_MINIMUM_VERSION. | ✓ | ✓ | |
| [From V4.11ag]<br>For HTTPS access the protocol versions TLS1.1 and TLS1.2 have been implemented. Previously only TLS1.0 was supported. | ✓ | ✓ | |
| [From V4.11de]<br>For the iGigaSwitch 1604, iGigaSwitch 1608 and iGigaSwitch 1612 switch types the Secure Mode can now be enabled via the F1 DIP switch on the front. Thus, this mode cannot be disabled via management access. | | ✓ | |
| [From V4.11df]<br>Does only apply to switches with a plugged-in memory card (MC):<br>Now the firmware of the switch can optionally be stored on the memory card. This option may be added via the Memory Card Mode. AES-256 encryption of the configuration will always be enabled.<br>**Manager – Extensions:**<br>In the Device Editor the Memory Card Mode parameter has been extended by the “Enabled with AES-256 encryption and Firmware storage” setting on the Agent tab. | ✓ | ✓ | ✓ |
| [From V4.11ao]<br>Does only apply to switches with a plugged-in memory card (MC):<br>Now the configuration of the switch can optionally be stored with an AES-256 encryption on the memory card. This option may be added via the Memory Card Mode.<br>**Manager – Extensions:**<br>In the Device Editor the Memory Card Mode parameter has been extended by the “Enabled with AES-256 encryption” setting on the Agent tab. | ✓ | ✓ | ✓ |
| **Firmware – Redundancy:** | | | |
| [From V4.11ab]<br>Does only apply to industrial switches with plugged-in memory card with MRP license:<br>Now detailed information on the MRP ring status are sent from the switch to the Switch Manager. These are shown in the Redundancy Details column of the Device List. | ✓ | ✓ | ✓ |
| **Firmware – SNMP:** | | | |
| [From V4.11ar]<br>A new version of the SNMP Private MIB and corresponding implementation in the firmware.<br>The following changes/extensions have been implemented:<br>- bmSwitchPortTable: object portActiveDefaultVlanId and portActiveVoiceVlanId added<br>- bmSwitchAdmin: object adminMemoryCardMode: enum mcEnabledWithAes256 and mcEnabledWithAes256AndFw added. | ✓ | ✓ | |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | ES3 | PRO3 | - |
| **Firmware – Bug Fixes:** | | | |
| [From V4.14P]<br>By enabling the VLAN Portmirror functionality on switch types 40 (iGigaSwitch 1604), 41 (iGigaSwitch 1608) and 42 (iGigaSwitch 1612), the switch reboots after a random period of time. | | ✓ | |
| [From V4.14A]<br>Does only apply to industrial switches of the iSwitch 542 type:<br>Under certain circumstances the yellow port LED indication was wrong for Twisted Pair Port 1.<br>Moreover, sporadically the link was not correctly set up, if the link partner did not support a Gigabit rate. | | ✓ | |
| [From V4.14M]<br>With the Security Scanner nmap a reboot of the switch could be provoked with the following option:<br>nmap -p 443 --script ssl-enum-ciphers | ✓ | ✓ | |
| [From V4.13ba]<br>It was not possible to assign the VLAN Name in the Web Interface. | ✓ | ✓ | |
| [From V4.13an]<br>When the VLAN Portmirror was enabled, the switch was set into a rebooting loop. | ✓ | ✓ | |
| [From V4.13ae]<br>In the Web Interface it was not possible to edit both the Username and the Password of the Admin Account. | ✓ | ✓ | |
| [From V4.11dp]<br>The request sent to a Radius Server has been increased from 100 bytes to 253 bytes. This is demanded by RFC 2865. | ✓ | ✓ | |
| [From V4.11dn]<br>After an MAC Bypass authentication the MAC table of the corresponding port was mistakenly not deleted after an EAP-LOGOFF. | ✓ | ✓ | |
| [From V4.11dr]<br>IGMP reports were also sent via Userports. This could result in problems with IGMP v1/v2. Now the IGMP reports are exclusively sent via the uplink. | ✓ | ✓ | |
| [From V4.11dq]<br>The source MAC address was not learned from incoming IEEE802.1X packets. As a result no authentication was performed. | ✓ | ✓ | |
| [From V4.11de]<br>Under certain circumstances in the Web Interface and with the Password Strength Checker enabled, a message was shown, that the password was not safe, although the password had been judged as safe. | ✓ | ✓ | |
| [From V4.11ab]<br>Does only apply to industrial switches with plugged-in memory card with MRP license:<br>Under certain circumstances the MRP Client reported that it had not found the Ring Manager, although the manager was correctly installed in the ring. This problem has been solved by the Ring Manager sending special status packets. | ✓ | ✓ | |
| [From V4.11aq]<br>Under certain circumstances with a high traffic load in the Management VLAN an Internal Management Warning indicating Code 101 was mistakenly sent. | ✓ | ✓ | |
| [From V4.11av]<br>Under certain circumstances packets in the Voice-VLAN were not correctly forwarded, if DHCP Snooping was enabled. | ✓ | ✓ | |
| [From V4.12A]<br>The ARP Cache Lifetime is now selected by a random generator in the range of 300…600 seconds, in order to prevent that too many ARP Requests are sent to the gateway. | ✓ | ✓ | |
| [From V4.12B]<br>If management authentication (SSH, SCP, TELNET, V.24, Manager) was performed via a RADIUS Server, passwords containing more than 16 characters might not have been correctly transmitted to the RADIUS Server. | ✓ | ✓ | |
| [From V4.12C]<br>Does only apply to switches from firmware version V4.11do:<br>Under certain conditions the Active Loop Protection did not disable all ports concerned. | ✓ | ✓ | |

## 2.9. Release V4.10C/V4.12C

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| Firmware family ➔ | ENHANCED/ SECURITY | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | ES3 | PRO3 | - |
| **Manager - Basic functions:** | | | |
| [from V4.03ab]<br>It is now possible to move a device again into the Category „Unassigned Devices“ after it had been assigned to a category. This goes either via Drag and Drop, or via „Add/Remove -> Move checked Devices to Unassigned Devices“. | | | ✓ |
| From V4.03ab]<br>The Link State on the “Global+Link State” tab was extended by the CLIENT-REMOVE-ALARM parameter. This parameter is also taken over as an alarm in the Alarms column of the Device List. | | | |
| [from 4.09aj]<br>A new software library has been implemented for the display of the Device-Lists. The new library needs less processing power and offers higher performance. For example, big device lists can be loaded quicker, or you can move quicker to a category listing a lot of devices. In addition to the higher performance, this new Grid allows an innovative operation/use, as well as a series of new functions like “Search and Group”. | | | ✓ |
| [from 4.09an]<br>The menu configure has been extended with the entry „Update Firmware of checked Devices simultaneously“. With this function it is possible to send a new Firmware up to 100 devices at the same time. The functions „Update Firmware by Device time client“ and „Don’t wait for switch reboot (use only for star topologies)“ are also available. | | | ✓ |
| [from 4.09bt]<br>New function implemented to clear “Non valid” industrial alarms. This function can be activated via the tab “Global” in the Preferences menu. | | | ✓ |
| [from V4.03ad]<br>New column „Active Links“ added in the Device-List. It shows the number of active Links of a Device. “Active Links” can be User as well as Uplink ports. | | | ✓ |
| [from V4.09aw]<br>The “Autodiscover Devices on local segments (Layer-2)” was extended by the Stop and Continue functions. Moreover, the Stop Autodiscover & Exit function was renamed to Close. | | | ✓ |
| [from V4.09aw]<br>Now devices can be switched into a Maintenance mode. For these devices in the Alarms column the Maintenance message is displayed. Even with an active alarm on this device, the corresponding Category will not be marked in red. | | | ✓ |
| **Manager - Bugfixes:** | | | |
| [from V4.03ab]<br>When choosing "Get Name/Location/Contact from CSV file by MAC Address (xxxxxxxxxx;Name;Location;Contact)" or "Get Name/Location/Contact/Domain from CSV file by MAC Address (xxxxxxxxxx;Name;Location;Contact;Domain)" in order to broadcast a Master-Config, the MAC-Address was not found in the CSV file | | | ✓ |
| [from V4.03aj]<br>The Category „Unassigned Devices“ was displayed as empty after a drag & drop of one or several devices from „Unassigned Devices“ into another category. | | | ✓ |
| [from V4.03ak]<br>The Master-Check Box for the „Password strength checker“ in the tab „Local Accounts“ was not displayed. As a result, it was not possible in the tab „Access Global“ to set the „Access policy“ on „Allow secure protocols and strong passwords only“. | | | ✓ |
| **Firmware – Basic functions:** | | | |
| [from V4.03ax]<br>The latency time to send Remote-Alarms has been significantly reduced and is now 6 ms on average and < 20ms in Worst-Case. These times are guaranteed for rings with up to 25 Switches.<br>In special cases (several Switches of the ring are sending simultaneously an alarm), the latency times were under specific conditions above 100ms. The sending/signaling of an alarm now occurs in a separate processor thread and via a quick Layer-2 protocol instead of via IPv4.<br>**Extensions in the Manager:**<br>In the Device Editor, the parameter „Remote Alarm IP Mode“ has been deleted from the tab „Function Input Alarms“. | ✓ | ✓ | ✓ |
| [from V4.03bb]<br>The Switch „GigaSwitch V3 TP(PD-F) SFP-I 48V ES3“ can be PoE-powered via the Uplink port and it can, now, forward the PoE voltage to up to 2 Class-1 or Class-2 end devices (altogether 8 Watt power consumption). In the past, it could forward to only one end device.<br>**Extensions in the Manager:**<br>In the Device Editor, in the tab „Alarms > Global Alarms“, the parameter „PoE Power Source“ has been completed with the mode "AF Power from TP uplink, max. 2x Class-1 or 2x Class-2 devices allowed (Port power limits forced to max. 4 W)". | ✓ | | |
| [from V4.03be]<br>In Link Layer Discovery Protocol LLDP, the maximum number of signs for the Port-ID and Chassis-ID is now higher (45 instead of 20). Very long ID‘s are now correctly displayed. | ✓ | ✓ | |
| [from V4.03bk]<br>It is now possible to activate DHCP Snooping for ports with the Link Type „Userport“ or „Userport with active Loop Protection“. This prevent from connecting a DHCP Server to these ports. If a DHCP Server is recognized, the Admin State of the corresponding port is switched on „Disabled by DHCP Snooping“.<br>**Extensions in the Manager:**<br>The tab „DHCP Relay Agent“ has been renamed in „DHCP Relay / Snooping“. And a new group „DHCP Snooping“ with the option „DHCP Snooping enable“ has been implemented in this tab. | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| [from V4.03bk]<br>For the Global LED Mode, we have implemented additional display modes:<br>• All LEDs green blinking<br>• Right LEDs red/blue blinking<br>**Extensions in the Manager:**<br>The „LED Setup“ on the tab „Global“ has also been extended with these 2 new display modes. | ✓ | | ✓ |
| [from V4.03be]<br>As long as there is no time received from a time server by using SNTP Client, every 30 seconds a request is send to the time server. This is now independent from the “Server request interval“. | ✓ | ✓ | |
| [from V4.03cd]<br>CLI test command for the function-input and alarm-outputs of industrial switches implemented. After direct electrical connection between one alarm output and the function input the CLI command "debug io-delay <alarm-output> <function-input>" can measure the total delay time of alarm-output-relay and function-input logic. If all electrical functions are working correctly the delay time must be less than 5ms. | ✓ | ✓ | |
| [from V4.03cg]<br>The maximum length of the user defined ports names has been extended from 15 to 64 characters.<br>**Extensions in the Manager:**<br>In the Device Editor the setting „Name Setup > Name“ has been modified accordingly on the Port tabs. | ✓ | ✓ | ✓ |
| [from V4.03cm]<br>The indication of the change source has been added to the Configuration Changed Alarm. Now it is possible to see whether a change in configuration was made via Manager, WEB, SNMP or CLI. | ✓ | ✓ | |
| [from V4.03dd]<br>After rebooting switches of the type "iSwitch 54x, 74x and 104x?" the SFP and fiber ports will be enabled delayed to securely prevent loops in ring topologies. If a ring topology using the redundancy protocols MSTP, RSTP or MRP is used it is strongly recommended that at least one of the two ring ports use a SFP or fiber port. | | ✓ | |
| [from V4.03dd]<br>Support for the switch types 40 (iGigaSwitch 1604), 41 (iGigaSwitch 1608) and 42 (iGigaSwitch 1612) implemented. These switches have 16 Gigabit ports, have been designed for harsh industrial environments and are equipped with an on-board management. The switches principally support all firmware functionalities, but the following features are not yet implemented in Firmware Version 4.10C: Multiple Spanning Tree, Link Layer Aggregation, DHCP Relay Agent, DHCP Snooping, Error counter, Bandwidth Limiter, Zero Loss. These features will be available in future releases. | ✓ | | |
| [from V4.09ak]<br>For the Link Layer Discovery Protocol MED (LLDP-MED) the Network Policy (TIA-1057) was expanded by the Layer 2 Priority Value and the Layer 3 DSCP Value both for Application Type Voice and Application Type Voice Signaling.<br>**Manager – Extensions:**<br>In the Device Editor the Layer 2 Priority Value and Layer 3 DSCP Value parameter are added to the Discovery tab. | ✓ | ✓ | ✓ |
| [from V4.09at]<br>A CLI command for deleting the ARP table has been implemented. | ✓ | ✓ | |
| [from V4.09aw]<br>For the “Shutdown Port if no Link” function a delayed disablement in case of a link down can be configured. The desired delay can be configured using the Client Remove Alarm feature. | ✓ | ✓ | ✓ |
| [from V4.09ay]‘<br>Does only apply to the 16 port industrial switches:<br>Support of the Aginode copper SFP has been implemented. Available rates: 10/100/1000Mbps. | ✓ | ✓ | |
| [from V4.10A]<br>Does only apply to the 16 port industrial switches:<br>Access to certain switch parameters is now possible using the IEC61850 protocol. For this implementation a KEMA conformance test report according to IEC 61850 Edition 2 is available.<br>**Manager – Extensions:**<br>In the Device Editor a new tab under the name of “Access IEC61850” has been implemented. | ✓ | ✓ | ✓ |
| **Firmware - Security:** | | | |
| [from V4.03be]<br>For ports with activated Portsecurity, the MAC Address 00:00:00:00:00:00 will now be rejected. Such invalid MAC Address is generated by defective PC Network cards when the PC is in Standby. | ✓ | ✓ | |
| [from V4.03cc]<br>SSL vulnerability "Poodle" fixed. For the integrated HTTPS server the SSLv3 protocol has been disabled. A connection is now only possible via TLSv1. | ✓ | ✓ | |
| [from V4.03cm]<br>A new alarm under the name of Port State Changed has been implemented. If enabled, this alarm will be sent after each change of the port state from Blocking to Forwarding or vice versa.<br>Manager – Extensions:<br>The Alarm Destination Table in the Device Editor has been extended by the Port State Changed parameter. | ✓ | ✓ | ✓ |
| [from V4.09ak]<br>A new parameter “MAC bypass Quiet Time” has been added to the 802.1X options. After receiving a Radius Reject, a new authentication is attempted no sooner than after expiration of the MAC Bypass Quiet Time.<br>**Manager – Extensions:**<br>In the Device Editor the “MAC Bypass Quiet Time” parameter has been added to the IEEE802.1x tab. | ✓ | ✓ | ✓ |
| [from V4.09ap]<br>Compatibility of the IEEE802.1X Supplicant (Port Security Mode setting: IEEE8021.X Supplicant with MD5 Challenge) for the authenticator of different vendors has been improved. | ✓ | ✓ | |
| [from V4.09av]<br>The IEEE802.1X authenticator now accepts all EAP versions (IEEE802.1X-2001, -2004 und -2010) | ✓ | ✓ | |
| [from V4.09ay]<br>For the integrated HTTPS server the TLS cipher suite with RC4 encryption has been disabled. The remaining cipher suits are using AES128 or AES256. | ✓ | ✓ | |
| [from V4.09az]<br>For the integrated HTTPS server a new RSA certificate with a SHA-256 signature has been installed. The corresponding CA certificate can be downloaded on the support portal. | ✓ | ✓ | |
| **Firmware - Redundancy:** | | | |

| | | | |
|---|---|---|---|
| [from V4.03cc]<br>Link Aggregation according to 802.1AX has been implemented. It is possible to configure up to eight LAG´s with the maximum of four member ports.<br>**Extensions in the Manager:**<br>In the Device Editor the new tab called “Link Aggregation“ has been implemented.- | ✓ | ✓ | ✓ |
| [from V4.03cc]<br>The MRP to Spanning Tree Network Coupling feature has been implemented. This function allows you to couple an MRP Ring redundantly to a Spanning Tree Topology.<br>**Manager – Extensions:**<br>In the Device Editor the function MRP to Spanning Tree Network Coupling has been added to the MRP tab. | | ✓ | ✓ |
| **Firmware - SNMP:** | | | |
| [from V4.03cg]<br>New SNMP protocol version called " SNMPv3 [Auth.-SHA] [Priv.-AES] with SNMPv1/SNMPv2c read/only access" implemented. This setting allows read/write access for SNMPv3 and read/only access for SNMPv1 und SNMPv2c.<br>**Extensions in the Manager:**<br>In the Device-Editor the parameter "SNMP Protocol Version“ has been extended with the setting “SNMPv3 [Auth.-SHA] [Priv.-AES] with SNMPv1/SNMPv2c read/only access" on the tab "Access SNMP“ | ✓ | ✓ | ✓ |
| [from V4.03cg]<br>New version of the Ne xans switch MIB: AGINODE-BM.MIB Version 4.02.<br>The following changes/extensions have been implemented:<br>`- bmSwitchInfo: object infoLastConfigChangeSource and infoLastPortStateChangeSource added`<br>`- bmSwitchAdmin: adminLedGlobalMode: enum ledGlobalModeGreenBlink and ledGlobalModeRedBlueBlink added.`<br>`- bmSwitchPortTable: portAdminState: dhcpSnoopingDisable(12) added`<br>`- bmSwitchPortTable: portSecurityForwardingState: enum portDhcpSnoopingDisable (19) added`<br>`- bmSwitchPortTable: portName: SIZE changed from 15 to 64 characters`<br>`- bmTraps: switchConfigurationChanged: object infoLastConfigChangeSource added`<br>`- bmTraps: trap portStateChanged added` | ✓ | ✓ | |
| **Firmware - Bugfixes:** | | | |
| [from V4.03au]<br>In both Port Security Modes "RADIUS allow two MAC addresses" and "RADIUS allow three MAC addresses“, the Guest VLAN was not correctly applied | ✓ | ✓ | |
| [from V4.03be]<br>On iSwitches with TP/SFP Combo port, the Speed/Duplex Mode of the TP port was set by mistake automatically to “Autoneg” after a reboot | ✓ | ✓ | |
| [from V4.03be]<br>While accessing via SNMP to the object „ifHighSpeed“ of the IF-MIB wrong values were shown for the current speed. | ✓ | ✓ | |
| [from V4.03be]<br>The CLI Command "in:terface <if-no> na:me [<string max. 15 chars>]" was not listed in the CLI Help. | ✓ | ✓ | |
| [from V4.03bn]<br>The CLI commands for setting the Admin and User passwords<br>`se:t {a:dmin\|u:ser} p:assword <string 1...xx chars>`<br>will now check whether the entered passwords contains invalid characters. | ✓ | ✓ | |
| [from V4.03cx]<br>While accessing via SNMP to the object „dot3StatsDuplexStatus“ of the IF-MIB the wrong value “Unknown” was shown if the current speed was 1000-FDX. | ✓ | ✓ | |
| [from V4.09af]<br>If in the Banner function two or more subsequent blanks were configured, these were wrongly shortened to one blank when output in the CLI and in WEB. | ✓ | ✓ | |
| [from V4.09am]<br>Now MAC addresses in the Voice VLAN are correctly blocked if authentication via IEEE802.1X and/or MAC bypass fails. | ✓ | ✓ | |
| [from V4.03ax]<br>The Guest VLAN was not correctly assigned in the "Radius allow 2 MACs" and "Radius allow 3 MACs" Port Security settings. | ✓ | ✓ | |
| [from V4.09ay]<br>The CLI command "show mac-address-table dynamic" incorrectly shows the MAC addresses of the uplink ports. This happens only if the switch was accessed via SNMPv1 in parallel. | ✓ | ✓ | |
| [from V4.09ay]<br>If using the industrial alarm function „Alarm from Remote Function Input“ the alarm outputs maybe activated without a corresponding function input trigger. This effect occurs only after an interruption of the supply voltage for the switch. | | ✓ | |
| [from V4.10A]<br>Under certain conditions the memory card configuration was not taken over when booting. The current FLASH configuration was loaded, instead. | ✓ | ✓ | |
| [from V4.10B]<br>Applies only to 'GigaSwitch V3' office switches:<br>The bandwidth limiter for broad- and multicast packets was not applied to unknown multicasts. | ✓ | ✓ | |
| [from V4.10B]<br>Applies only to industrial switches:<br>The configuration and status display for the input/output signals was not completely implemented within the CLI und WEB interfaces. | ✓ | ✓ | |
| [from V4.10C]<br>Applies only to industrial switches with 16 ports:<br>Under certain conditions the transmitting of the input voltages S1 and S2 to the manager has been wrong and was shown as 0 Volt. | | ✓ | |
| [from V4.10C]<br>Applies only to industrial switches with 16 ports:<br>The displaying of the “PoE State” in the WEB interface was incomplete, when a PoE adapter with 8 or 12 channels was installed. | | ✓ | |

| | | | |
|---|---|---|---|
| [from V4.10C]<br>Applies only to industrial switches with 16 ports:<br>The CLI command “help” showed some functionalities that were not supported by the switch type. | | ✓ | |
| [from V4.10C]<br>Applies only to industrial switches:<br>The MRP protocol could be activated even if there was no memory card with MRP license installed. | | ✓ | |

## 2.10. Release V4.02

## 2.10.1. Release V4.02B

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| **Firmware family ➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Firmware - Bugfixes:** | | | |
| [from V4.02B]<br>In the CLI console, entering different show commands, the Port Description of the Uplink Ports was not complete because the text was longer than ten signs (max displayed signs). For example, the following text „FO-VARIO-1“ was displayed instead of „FO-VARIO-10“. The Port Descriptions have now been re-written with each max. 10 signs. | ✓ | ✓ | |
| [from V4.02B]<br>The function Tagging Ethertype 9100 and 9200 (Q-in-Q Function) of the Industrial Switch „iSwitch 1043“ was not working properly. The problem has been fixed and the function extended. In addition to this, the Q-in-Q Function has also been implemented in the Industrial Switch „iGigaSwitch 541/542“. It is now possible to apply different Customer Ports to different Provider Ports.<br>**Extensions in the Manager:**<br>The parameter „Tagging Ethertyp“ has been moved from the tab „Global“ to the tab „VLAN Table“. | ✓ | ✓ | |
| [from V4.02B]<br>Problem during Reboot and Update of the Switch on the test bay of the manufacturer has been solved. | ✓ | ✓ | |

## 2.10.2. Release V4.02

| Switch family➔ | Office | Industry | Manager |
|---|---|---|---|
| **Firmware family ➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Manager – Basic Features:** | | | |
| [from V4.01ar]<br>During the installation English, German or French can be selected as the basic Manager language. After the successful installation the language can be switched on the fly under Extras>Preferences. The names of the individual parameters in the Device Editor continue to be indicated in English, because a translation of network terms is not practical. | | | ✓ |
| [from V4.01ar]<br>The switches in the Device List can now be grouped in so-called “Categories” using a freely definable tree structure. Existing Device Lists of Manager Version V3.xx can be imported in any user-defined Category. | | | ✓ |
| [from V4.01cb]<br>The width of the Device List columns can be adjusted via the Adjust Column Size button (below the Device List) to fit the contents of the cells. A permanent automatic adjustment of the width has been disabled for performance reasons and the corresponding “Adjust Column size automatically” setting removed from the Preferences menu. | | | ✓ |
| [from 4.01au]<br>The following setting has been added to the NexMan Manager Preferences: “Protocol version for WEB / CLI access:” The following options are offered:<br>IPv6 first, then IPv4 (default)<br>IPv4 only<br>IPv6 only | | | ✓ |
| [from 4.01av]<br>A new tab named “IPv4 / IPv6 Setup” has been added to the Device Editor. The IPv4 parameter settings have been moved from the “Agent” tab to the new tab. In addition, the IPv6 parameters can be configured there. | | | ✓ |
| [from 4.01ar]<br>A column “IPv6 Address” has been added to the Device List. This column can be displayed via the Extras > Preferences > Device List menu. | | | ✓ |
| [from 4.01ar]<br>A column “IPv6 Link Local Address” has been added to the Device List. This column can be displayed via the Extras > Preferences > Device List menu. | | | ✓ |

| | | | |
|---|---|---|---|
| [from 4.01ar]<br>A column “IPv6 Address” has been added to the Layer-2 Autodiscovery. | | | ✓ |
| [from 4.01ar]<br>The IGMP Multicast tab in the Device Editor was renamed to Multicast. At the same time the new MLDv1/v2 settings have been added. | | | ✓ |
| [from 4.01bs]<br>In the Alarm Destination Table now an IPv6 address can be entered as a Destination IP in addition to the IPv4 address. | | | ✓ |
| [from 4.01bl]<br>NexMan was extended by an error logging function. This feature can be configured in the NexMan Preferences. | | | ✓ |
| [from 4.01bi]<br>In case of a faulty SCP communication now the SCP Return Code is written in the Manager’s log. | | | ✓ |
| [from 4.01]<br>The Alarm Destination Table in the Device Editor has been extended by the Port Error Disabled parameter. | | | ✓ |
| [from 4.01bj]<br>NexMan was extended by the parallel polling of several switches contained in the Device List. In particular for a large number of devices this provides the advantage that the switch status will be refreshed more quickly. This simultaneous polling can be configured under Preferences -> Device List. | | | ✓ |
| [from 4.01az]<br>Now an Access List for IPv6 addresses can be created on the Access Global tab. | | | ✓ |
| [from 4.01ax]<br>On the SNTP Setup tab now an IPv6 address can be entered as a Time Server IP in addition to the IPv4 address. | | | ✓ |
| [from 4.01cd]<br>Now Local Logging can be read via SCP into the data base. The right-click menu of the Device List as well as the Configure menu of the Device List/Editor now provide the following option: ”Read Local Logging messages of checked Device into Database (via SCP)”. The file is saved into the data base folder in the “<ip-adresse>_local.log” format. | | | ✓ |
| [from 4.01az]<br>Under the Global Settings of the Manager’s Preferences it is now possible to enter different time intervals for the “Timeout for writing config or firmware”. | | | ✓ |
| [from 4.01bs]<br>Now on the RADIUS Global Auth., RADIUS Management Auth. and RADIUS Accounting tabs four Radius servers can be configured each. | | | ✓ |
| [from 4.01bs]<br>A new Radius State tab was implemented. The state indicators of the individual Radius servers have been moved from the MAC+Security State tab to the new tab. At the same time the states for the added Radius servers have been added. | | | ✓ |
| **Manager - Bugfixes:** | | | |
| [from V4.01ck]<br>During a long time usage of the manager without restarting a crash with the error message “Error creating window handle” rarely occurred. This problem has been fixed. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V.4.01bb]<br>It is now possible to define a banner. The banner will be shown before logging in the CLI or Web interface.<br>**Manager – Extensions:**<br>A new tab named “Banner” has been added to the Device Editor. | ✓ | ✓ | ✓ |
| [from V.4.01bb]<br>For security reasons the default “Manager Authentication Mode” was changed from „UDP/TFTP – No authentication (Ignores Username and Password)“ to „SCP – Use SCP authentication mode setting“ | ✓ | ✓ | |
| [from V.4.01ba]<br>For the Local Logging the Local Logging State has been implemented. The status can assume the following values: „Disabled“, „Empty“, „Entries present“ und „Log overflow“. Additionally the count of entries will be shown.<br>**Manager – Extensions:**<br>On the Global+Link State tab a Local Log State indicator as well as the count of the messages has been implemented. The Device-List has been extended by the optional “Local Log” column. This column can be displayed, if required, via the menu “Extra > Preferences > Device-List”. | ✓ | ✓ | ✓ |
| [from V4.01ba]<br>The IPv6 protocol according to IPv6 Forum Phase 2 Specification (Gold Logo) was implemented. Now the switch can be accessed via IPv6 using Ping, SNMPv1/v2/v3, Telnet, SSH, HTTP and HTTPS. Requests by the switch, such as SNMP traps, Syslog messages and RADIUS requests, can now be executed via IPv6, too.<br>**Manager – Extensions:**<br>All IPv6 parameters can be configured using the Device Editor. The Device List and the Layer-2 Autodiscover List have each been extended by two columns for the IPV6 Link Local Address and the IPV6 Address. IPv6 access to the switch is possible via the Configure menu. | ✓ | ✓ | ✓ |
| [from V4.01bp]<br>The response times to ICMP Ping Requests have been significantly improved. Now the average response time is 0.5ms and the worst-case time is about 5ms. | ✓ | ✓ | - |
| [from V4.01cw]<br>Now it is possible via the Local Logging Mode to specify whether the oldest entries shall be overwritten in the log in case of overflow or whether logging shall be stopped. Moreover local logging can be disabled globally.<br>**Manager – Extensions:**<br>In the Device Editor the Local Logging Mode parameter has been implemented on the Alarm Destinations tab. | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| [from V4.01dg]<br>For switches with functional input it is now possible to configure whether the remote alarm packets shall be sent via IPv4 or IPv6.<br>**Manager – Extensions:**<br>In the Device Editor the IP Address Mode parameter has been implemented on the Function Input Alarms tab. | ✓ | ✓ | ✓ |
| [from V4.01dg]<br>The refresh time for the ARP cache table was increased to 4 hours. This will significantly reduce the number of ARP requests in the networks, in particular if there are many switches in the same subnet. | ✓ | ✓ | - |
| [from V4.01et]<br>If DHCP is enabled, now the current lease times are indicated via CLI ("show dhcp" command) and via the WEB interface (Device Info tab). | ✓ | ✓ | - |
| [from V4.01fk]<br>Now TFTP download with DHCP/BOOTP can be globally disabled in order to prevent a configuration file from loading when rebooting the switch. This is particularly helpful, if a configuration file may only be loaded when first booting after an installation, but DHCP shall continue to be enabled.<br>**Manager - Extensions:**<br>In the Device Editor the DHCP/BOOTP Download Mode parameter has been implemented on the Agent tab. | ✓ | ✓ | ✓ |
| [from V4.01gp]<br>The configured names for Contact and Domain will be send to manager via UDP status polling.<br>**Manager – Extensions:**<br>The Device-List has been extended by the optional "Contact" and "Domain" columns. These columns can be displayed, if required, via the menu "Extra > Preferences > Device-List". | ✓ | ✓ | ✓ |
| [from V4.01gp]<br>The configured redundancy parameters and the redundancy state of the particular port will be send to manager via UDP status polling.<br>**Manager – Extensions:**<br>The Device-List has been extended by the optional "Redundancy Overview" column. This column can be displayed, if required, via the menu "Extra > Preferences > Device-List". | ✓ | ✓ | ✓ |
| **Firmware - Portsecurity:** | | | |
| [from V4.01dg]<br>For requests to the Radius server a Server Request Algorithm has been implemented. The following settings are possible: strict-priority, round-robin, parallel<br>**Manager – Extensions:**<br>Now the Server Request Algorithm can be configured on the RADIUS Global Auth. tab. | ✓ | ✓ | ✓ |
| [from V4.01dg]<br>For the MAC addresses learned via Portsecurity a new ageing time was introduced under the description of "Portsecurity ageing time for PC behind IP-Phone". This ageing time does only apply to terminal devices connected behind an IP phone. The precondition is that the Portsecurity mode is set to "IEEE802.1X PC+Voice allow two MAC addresses" and that a MAC address was detected on the port in the voice VLAN.<br>**Manager – Extensions:**<br>In the Device Editor the "Portsecurity ageing time for PC behind IP-Phone (minutes)" parameter has been implemented on the Security > Security Setup tab. | ✓ | ✓ | ✓ |
| [from V4.01cw]<br>Now a delayed shut-down can be configured for the "Shutdown Port if no Link" function. This will delay the checking of the link signal by 30 seconds after a reboot. Among others this feature will prevent the port from being disabled after a firmware update.<br>**Manager – Extensions:**<br>In the Device Editor the setting "Check Link permanently delayed" has been added to the "Shutdown Port if no Link" parameter on the Port tabs. | ✓ | ✓ | ✓ |
| **Firmware - Redundancy:** | | | |
| [from V4.01dk]<br>For analysing spanning tree problems it is now possible to write debugging data into the internal log. The following log settings are available: "Overwrite old entries on overflow", "Stop logging on overflow" and "Disable local logging globally".<br>**Manager – Extensions:**<br>In the Device Editor the Debugging mode has been added to the Spanning Tree tab. The Local Logging Mode has been added to the Alarm Destination Table tab. | ✓ | ✓ | ✓ |
| [from V4.01dk]<br>For the Spanning Tree Port mode the "Disabled (BPDU disables Port)" mode has been implemented. When selected, the corresponding port will not send any BPDU packets, and received BPDU packets result in the port being disabled. In this case BPDU-DISABLED will be indicated as the port's link status and a Port Error Disable alarm will be sent. Optionally, disabled ports can automatically be re-enabled after a settable "Re-Enable Time for BPDU-Disabled Ports". The time value can be set in the range from 1 to 60000 seconds.<br>**Manager – Extensions:**<br>In the Device-Editor the Disabled (BPDU disables Port) setting has been added to the Port Spanning Tree Mode on the Spanning Tree tab. And on the Spanning Tree tab the "Re-Enable Time for BPDU-Disabled Ports" parameter has been implemented. | ✓ | ✓ | ✓ |
| [from V4.01dk]<br>Ports, for which the spanning tree is disabled, will now additionally block outgoing PVST+ packets. However, incoming PVST+ packets will not be blocked and forwarded to all ports for which the spanning tree is enabled. But if the reception and forwarding of PVST+ packets shall be prevented, the "Port Spanning Tree Mode" of the corresponding port should be set to "Disabled (BPDU disable Port)". In this case the port will be disabled as soon as a spanning tree packet is received. Note: If spanning tree is globally disabled, all spanning tree packets are principally forwarded to all ports. | ✓ | ✓ | |

| | | | |
|---|---|---|---|
| [from V4.01ga]<br>For the Spanning Tree Port mode the “Enabled (Ring Loop Protection)” mode has been implemented. When selected, for the corresponding port a periodic check is executed as to whether a ring loop exists. This security feature prevents that a loop is generated in the ring due to a fault in the spanning tree topology calculation.<br>**Manager – Extensions:**<br>In the Device-Editor the Enabled (Ring Loop Protection) setting has been added to the Port Spanning Tree Mode on the Spanning Tree tab. | ✓ | ✓ | ✓ |
| **Firmware - SNMP:** | | | |
| [from V4.01fa]<br>New SNMP OIDs and traps implemented, MIB version AGINODE-BM-MIB V4.01. | ✓ | ✓ | |
| **Firmware – Bug Fixes:** | | | |
| [from V4.01bp]<br>If the Portsecurity mode was set to IEEE802.1X without MAC bypass, the port always wrongly remained in the Unsecure VLAN after an IEEE802.1X Authentication Timeout. Now the port is correctly moved into the Guest VLAN (if a Guest VLAN is configured). | ✓ | ✓ | - |
| [from V4.01dc]<br>Does only apply to switches from firmware version V3.67ha:<br>The spanning tree algorithm was disrupted by polling the SNMP BRIDGE MIB und the “dot1dStpPortDesignatedRoot” and/or “dot1dStpPortDesignatedBridge” OIDs. Under certain conditions this resulted in an undefined blocking of individual ports. | ✓ | ✓ | - |
| [from V4.01de]<br>After rebooting the switch it might have happened under certain conditions that a request to renew the VLAN and IP parameters was wrongly displayed in the CLI and WEB interface. | ✓ | ✓ | - |
| [from V4.01ea]<br>After an uptime of “49 days : 17 hours : 2min” (or multiples thereof) a malfunction of the spanning tree algorithm and of internal test routines could occur. As a result, alarms of the “New Root”, “Topology Change” and/or “Internal Management Warning” type might have been generated and the network connection was sporadically interrupted for a maximum of 2 seconds. | ✓ | ✓ | - |
| [from V4.01fa]<br>If the Multiple Spanning Tree protocol was activated and a non-conforming MSTP BPDU was received, this could lead to a reboot of the switch. | ✓ | ✓ | - |

## 2.11. Release V3.68

| **Switch family➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| **Firmware family ➔** | **ENHANCED/ SECURITY** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **ES3** | **PRO3** | **-** |
| **Manager – Basic Features:** | | | |
| [from V3.67]<br>Now it is possible to read the CLI-Configuration with all parameters from the Device-List into the database. This is equivalent to the “show run all” CLI command. This process is possible at two positions:<br>a) With a right-click of your mouse on the desired switch and selecting “Read CLI-Config from Device (with all parameters)”.<br>b) Under „Configure -> Read CLI-Config of checked Devices into Database (with all parameters)”. | | | |
| [from V3.67bu]<br>The Device-List has been extended by the optional “Time scheduled firmware update” column. This column can be displayed, if required, via the menu “Extra > Preferences > Device-List”. | | | |
| [from V3.67bu]<br>The Device-List has been extended by the optional “Port Security Setup” column. This column can be displayed, if required, via the menu “Extra > Preferences > Device-List”. | | | |
| [from V3.67bu]<br>In the Device Editor now an Inventory-List can be created containing the current SFP information: Port Description, Vendor Name, Part Number and Serial Number. The precondition is that the respective switch can be reached. The entry is located under „Inventory -> Create Excel Inventory-List for checked Devices from Database (including Device SFP information)”. | | | |
| [from V3.67ae]<br>NexManV3 has been updated from .Net 2.0 to .Net 4.0. If this software is not installed on your computer, you can download it via the Microsoft homepage free of charge. | | | |
| [from V3.67ae]<br>Now in the Device-Editor the MAC addresses of the connected terminal devices can be copied into the PC’s clipboard.<br>This can be done at two positions in the Device-Editor by right-clicking with your mouse:<br>a) On the “MAC+Security State” tab in the “MAC Address 1/2/3” columns.<br>b) In the “Show > MAC Address Table” menu in the “MAC Address” column. | | | |
| [from V3.67ae]<br>In the Device Editor the new “Function Input Alarms” tab has been added under “Alarms“. | | | |
| [from V3.67ae]<br>In the Manager under “Preferences > Global” the item “Don’t save Config to Database” has been added. If this setting is activated, no binary and CLI configurations will be saved in the database. | | | |

| | | | |
|---|---|---|---|
| [from V3.67ae]<br>In the Device-List the MAC address and/or the IP address of the switch can now be copied into the PC's clipboard. To do so, select the desired switch by right-clicking your mouse first and then select the corresponding "Copy MAC/IP… to clipboard" menu item. | | | |
| **Manager – Bug Fixes:** | | | |
| [from 3.67bu]<br>In the Master Editor the "Password Encryption Mode" was automatically checked and greyed out, when Admin or User Password was selected under "Local Accounts". At the same time the checkmark at Admin or User Password was counted wrongly. Both problems have been fixed. | | | |
| [from V3.67ad]<br>When "Write Config to Device" was executed in the Basic Configurator, the "Trunk Port" set and the "Mgmt VLAN" were not imported. | | | |
| | | | |
| **Firmware – Basic Features:** | | | |
| [from V3.67eg]<br>Now the Manager authentication, die import of the configuration and the firmware update can alternatively be performed via an encrypted SCP connection.<br>**Manager – Extensions:**<br>In the Device-Editor the "Manager Authentication Mode" parameter on the "Access Global" tab was extended by the "SCP – Use SCP authentication mode setting" setting. In addition the Manager access mode in the "Extras > Preferences" menu on the "Access" tab has been extended by the "SCP only" and "UDP/TFTP first, then SCP" entries. | | | |
| [from V3.67cd]<br>Via the new "Shutdown Port if no Link" function it is possible to automatically disable a port in case of a missing link signal. If no link is available at the moment of checking, the respective port will be permanently disabled. This is done by switching the Admin State to "Disabled". This setting will be kept also after rebooting the switch.<br>The following settings are possible:<br>• Disabled<br>• Check Link one time<br>• Check Link permanently<br>**Manager – Extensions:**<br>In the Device Editor the "Shutdown Port if no Link" parameter has been implemented on the port tabs. | | | |
| [from V3.67cd]<br>On the "Alarm Destination" tab the "Function Input Alarm" and "Configuration Changed Info" alarms have been added. | | | |
| [from V3.67cf]<br>Via the Reset function in WEB, CLI and Manager now the following additional reset actions can be performed:<br>• Reset Total Boots Counter<br>• Reset Total Operation Time<br>In addition, in the Manager the following reboot commands can be triggered:<br>• Reboot with Factory Default (Except IP Parameters)<br>• Reset Port Counters<br>• Reset Total Boots Counter, Total Operation Time and Local Logging<br>• Reset Local Logging<br>**Manager – Extensions:**<br>In the Device Editor the "Reset Action" parameter has been implemented on the "Agent" tab. | | | |
| [from V3.67cd]<br>The LED Setup function allows you to globally configure the display mode of the switch LEDs. The following display modes can be set:<br>• Standard<br>• All LEDs Off<br>• All LEDs Off, except Mgmt LED<br>• All LEDs On<br>**Manager – Extensions:**<br>In the Device Editor the "LED Setup" parameter has been implemented on the "Global" tab. | | | |
| [from V3.67ca]<br>The Memory Card Mode allows you to disable the memory card features. The following settings are available:<br>• Enabled<br>• Disabled<br>• Permanently Disabled<br>**Manager – Extensions:**<br>In the Device Editor the "Memory Card Mode" parameter has been implemented on the "Agent" tab. | | | |
| [from V3.67cb]<br>For switches supporting the "Energy Efficient Ethernet (EEE)" now the EEE status is indicated in Manager, WEB and CLI. The EEE mode is only enabled, if the connected terminal device also supports EEE. In this case after "Link State" additionally "/EEE" is indicated in WEB and CLI.<br>**Manager – Extensions:**<br>In the Device-Editor the "EEE State" column was added to the "Global+Link State" tab. This column is only displayed, if the respective switch supports EEE. | | | |

| | | | |
|---|---|---|---|
| [from V3.67ce]<br>Now the Manager authentication, die import of the configuration and the firmware update can alternatively be performed via an AES encrypted SNMPv3 connection.<br>**Manager – Extensions:**<br>In the Device-Editor the “Manager Authentication Mode” parameter on the “Access Global” tab has been extended by the “SNMPv3 – Local Accounts” setting. Furthermore the “Manager Access Mode” basic setting has been added to the “Extras > Preferences” menu on the “Access” tab. | | | |
| [from V3.67ch]<br>The local Admin and User Accounts passwords can now be saved as an SHA1 hash alternatively to the MD5 hash.<br>**Manager – Extensions:**<br>In the Device-Editor the “Password Encryption Mode” parameter on the “Local Accounts” tab has been extended by the “SHA1 Hash” setting. | | | |
| [from V3.67he]<br>Support for switch types 62, 63 and 64 (GigaSwitch V3), 66 (FiberSwitch 1000 V3), 67 (FiberSwitch 100 V3), 70 and 71 (GigaSwitch 641 Desk) has been implemented. These switches are equipped with an on-board management generally supporting the complete set of functions of all firmware features. | | | |
| [from V3.67hf]<br>Check for minimum required firmware version implemented. This will prevent a firmware downgrade to a version that doesn’t support this particular switch type. | | | |
| **Firmware - Portsecurity:** | | | |
| [from V3.67bm]<br>When a RADIUS Access-Accept is received, now additionally the “device-traffic-class=voice” Cisco attribute is interpreted. If this attribute is set, the received VLAN-ID is interpreted as a Voice-VLAN and accordingly set as a tagged VLAN. | | | |
| [from V3.67bm]<br>Upon successful authentication per IEEE802.1X MAC Bypass now a fallback to IEEE802.1X can be configured. This function is particularly interesting, if the connected terminal enables its IEEE802.1X function only after a successful MAC authentication (e. g. during the first filling of PCs).<br>**Manager – Extensions:**<br>In the Device Editor the “RADIUS MAC bypass” parameter has been extended accordingly on the “IEEE802.1X” tab. | | | |
| **Firmware - Redundancy:** | | | |
| [from V3.67eg]<br>A new Manager Mode with a so-called “Ring Port 1 Priority” has been implemented for the MRP redundancy protocol. Unlike in the Standard Manager Mode, for a closed ring topology Ring Port 1 is generally switched to “forwarding” and Ring Port 2 to “blocking”.<br>**Manager – Extensions:**<br>In the Device-Editor the “Admin Role” on the “MRP” tab has been extended by the “MANAGER (with Ring Port 1 Priority)” setting. | | | |
| [from V3.67ha]<br>The Rapid Spanning Tree (RSTP) and Multiple Spanning Tree (MSTP) protocols have been switched to the current IEEE 802.1Q -2011 standard.<br>In addition, for both protocols now a detailed debugging function is available per CLI.<br>The corresponding CLI command reads:<br>`# de:bug s:tp {e:nable\|de:tail\|di:sable}`<br>`Print debug information for Spanning-Tree protocol to console.`<br>`Use parameter 'detail' to print also detailed packet information.`<br>`Console inactivity timeout temporarily set to 24h until next keystroke.` | | | |
| [from V3.67ha]<br>The Rapid Spanning Tree (RSTP) and Multiple Spanning Tree (MSTP) protocols have been switched to the current IEEE 802.1Q -2011 standard. | | | |
| [from V3.67ha]<br>The current Multiple Spanning Tree status for all configured instances is now displayed in the WEB interface. Previously this was possible via Manager and CLI only. | | | |
| **Firmware - Command Line Interface (CLI):** | | | |
| [from V3.67ef]<br>Now the console logout time can be configured as follows:<br>`# co:nfig console-l:ogout-timeout (5...65535)`<br>`Sets the inactivity timeout for the cli console in seconds.`<br>**Manager – Extensions:**<br>In the Device Editor the “Console logout time (seconds)” parameter has been added to the “Access Global” tab. | | | |
| **Firmware - WEB:** | | | |
| | | | |
| **Firmware - SNMP:** | | | |
| [from V3.67ce]<br>New SNMP OIDs and traps implemented, MIB version AGINODE-BM-MIB V3.98:<br>- bmSwitchAdmin: adminAlarmNameM1, adminAlarmNameM2, adminFunctionInputNameF1<br>- bmSwitchAdmin: adminMemoryCardMode<br>- bmSwitchPortTable: portPrioDot1p und portPrioIp<br>- bmSwitchInfo: infoFunctionInputStateF1 and infoTotalConfigChanges<br>- bmTraps: trap switchFunctionInputAlarm and switchConfigurationChanged | | | |

| | | | |
|---|---|---|---|
| [from V3.67ce]<br>Compatibility with several SNMPv3 management systems improved. Previously the SNMPv3 Discover process was occasionally aborted by Manager, because the switch did not accept zero values for "msgAuthEngineTime" and "msgAuthEngineBoots", if Privacy was enabled. | | | |
| [from V3.67ch]<br>SNMPv3 traps implemented. Here a name and a password for sending the traps can be configured.<br>**Manager – Extensions:**<br>In the Device Editor the "Select Destination Type" parameter on the "Alarm Destinations" tab has been extended by the "SNMPv3 Trap" option. Moreover the "SNMPv3 Trap Setup" group has been implemented on the "Access SNMP" tab. | | | |
| [from V3.67ch]<br>Now access per SNMPv3 is also possible per AES encryption as an alternative to DES encryption.<br>**Manager – Extensions:**<br>In the Device-Editor the "SNMP Protocol Version" parameter on the "Access SNMP" tab has been extended by the "SNMPv3 [Auth.-MD5][Priv.-AES-128]" and "SNMPv3 [Auth.-SHA][Priv.-AES-128]" settings. | | | |
| [from V3.67ch]<br>Now for access per SNMPv3 the passwords for Authentication and Privacy can be set separately.<br>**Manager – Extensions:**<br>In the Device Editor the "Privacy Password" parameter has been implemented on the "Access SNMP" tab. | | | |
| **Firmware – Bug Fixes:** | | | |
| [from V3.67ca]<br>If a CLI configuration page was loaded via TFTP and this page contained the<br>`vlan-table delete 1`<br>command, under certain conditions the switch performed a cold start. In this case the configuration loaded was not imported. | | | |
| [from V3.67ca]<br>When accessing the Q-BRIDGE-MIB through the "ARP-GUARD" security tool, the switch was occasionally rebooted, if the MAC table contained the 00: 00: 00: 00: 00: 00 MAC address. | | | |
| [from V3.67ca]<br>If RADIUS Accounting was enabled in combination with "Discover IP Address", the management froze under certain conditions, which required a hardware reset of the switch. | | | |
| [from V3.67ha]<br>The CLI debug function for Multiple Spanning Tree (MSTP) occasionally froze. This problem was fixed. | ✓ | ✓ | - |

## 2.12. Release V3.66

Firmware families marked with (1) are no longer supported since Firmware-Release V3.66. The other firmware families SECURITY, ENHANCED/SECURITY and I-PROFESSIONAL are freely available now, so that it is possible to make a free upgrade to these families.

## 2.12.1. Release V3.66G

| **Switchfamilie ➔** | **Office** | | | | **Industry** | | **Manager** |
|---|---|---|---|---|---|---|---|
| **Firmwarefamilie ➔** | **WEB (1)** | **SNMP/ TELNET/ WEB (1)** | **SECURITY (2)** | **ENHANCED/ SECURITY (2)** | **I-BASIC (1)** | **I-PROFES SIONAL (2)** | **NexManV3 Switch Manager** |
| **Bundle Kennung ➔** | **-** | **-** | **-** | **ES3** | **-** | **PRO2 PRO3** | **-** |
| **Firmware - Bugfixes:** | | | | | | | |
| Applies only to devices with Hardware Management version HW2:<br>Under certain circumstances it was possible that the Switch sends faulty RSTP BPDUs packets. By receiving these packets the neighbour switches send a sporadically "topology change" alarm. | | | | ✓ | | ✓ | - |

## 2.12.2. Release V3.66F

| **Switchfamilie ➔** | **Office** | | | | **Industry** | | **Manager** |
|---|---|---|---|---|---|---|---|
| **Firmwarefamilie ➔** | **WEB (1)** | **SNMP/ TELNET/ WEB (1)** | **SECURITY (2)** | **ENHANCED/ SECURITY (2)** | **I-BASIC (1)** | **I-PROFES SIONAL (2)** | **NexManV3 Switch Manager** |
| **Bundle Kennung ➔** | **-** | **-** | **-** | **ES3** | **-** | **PRO2 PRO3** | **-** |

| Switchfamilie ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmwarefamilie ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY (2) | ENHANCED/ SECURITY (2) | I-BASIC (1) | I-PROFESSIONAL (2) | NexManV3 Switch Manager |
| Bundle Kennung ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Firmware - Bugfixes:** | | | | | | | |
| Applies only to devices with Hardware Management version HW2:<br>If there was a SNMP Get-Next-Request that contains at least 15 OIDs done on a switch that had Spanning Tree enabled the BPDUs of this switch were send delayed. If this Get-Next-Request was sent at shot time intervals it could cause that the neighbour switch did not recognized this switch anymore and sends "New Root" or "Topology Change" alarm. | | | | ✓ | | ✓ | - |

## 2.12.3. Release V3.66E

| Switchfamilie ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmwarefamilie ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY (2) | ENHANCED/ SECURITY (2) | I-BASIC (1) | I-PROFESSIONAL (2) | NexManV3 Switch Manager |
| Bundle Kennung ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Firmware - Bugfixes:** | | | | | | | |
| Applies only to devices with Hardware Management version HW2:<br>If a CLI configuration file that contains the following command was loaded via TFTP it could cause a cold start under certain circumstances:<br>vlan-table delete one<br>In this case the loaded configuration file was not assumed<br>Note:<br>The appropriate bug fixing for Management Hardware Version HW3 was performed in pre-release version V3.67cm (or higher). | | | ✓ | ✓ | | ✓ | - |

## 2.12.4. Release V3.66D

| Switchfamilie ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmwarefamilie ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY (2) | ENHANCED/ SECURITY (2) | I-BASIC (1) | I-PROFESSIONAL (2) | NexManV3 Switch Manager |
| Bundle Kennung ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Firmware - Bugfixes:** | | | | | | | |
| Applies only to devices with Hardware Management version HW0, HW1 and HW3:<br>Depending on the web browser version and settings the access to the web interface of the switch was broken after a few repeatedly access. | | | ✓ | ✓ | | ✓ | - |
| Applies only to 'GigaSwitch V3' switches:<br>Under certain circumstances it was possible that the switches reboots. This dependents on the load of the network traffic in the management VLAN. | | | ✓ | ✓ | | ✓ | - |

## 2.12.5. Release V3.66C

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY | ENHANCED/ SECURITY | I-BASIC (1) | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Manager - Extensions:** | | | | | | | |
| When the installation programme for the Manager is executed, it will be checked whether a Manager version is already installed. If yes, it is possible to select, whether the existing Manager shall be updated only. All further queries of the installation programme will be skipped and all settings preserved. | | | | | | | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY | ENHANCED/ SECURITY | I-BASIC (1) | I-PROFES SIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| In the Device Editor the Show buttons, which previously were selectable via the 'Global+Link State' and 'MAC+Security State' tabs, have been shifted to the new 'Show' menu. This allows you to execute the Show functions across all tabs. | | | | | | | ✓ |
| In the Device List the 'Read CLI-Config from Device' option has been implemented in the right-click menu. This function allows you to read the CLI configurations of the selected switch. The configuration will automatically be saved in the database directory under the name of xxx_xxx_xxx_xxx.cfg. | | | | | | | ✓ |
| In the Device List the 'Read CLI-Config from Database' option has been implemented in the right-click menu. This function shows the CLI configurations of the selected switch which were last read and stored in the database. | | | | | | | ✓ |
| When writing the config to the switch using the '[Write Config to Device]' or 'Copy Master-Config to checked devices' command, now it is possible to select via the 'Don't read back Config after writing Device' function, whether the modified config shall be read back after writing. This might make sense, e. g. if, after writing the config, the switch cannot be reached any longer under the existing IP address (e. g. because the VLANs have been changed and the switch obtains a new IP address via DHCP in the new management VLAN). Previously in those cases the timeout of the Manager had to be waited for. | | | | | | | ✓ |
| **Manager – Bug Fixes:** | | | | | | | |
| Under certain circumstances, on the 'DHCP Relay Agent' tab the 'Role' setting was not taken over after executing 'Write Config to Device'. | | | | | | | ✓ |
| **Firmware – Basic Features:** | | | | | | | |
| [From V3.65aa]<br>Does only apply to the 'GigaSwitch 542 Desk' and 'iGigaSwitch 542' switch types:<br>Now for Port 1 (VARIO-1) the 'ECO 10/100' speed/duplex mode can be set. | | | ✓ | ✓ | | ✓ | ✓ |
| [From V3.65aa]<br>The number of reboots since the manufacture of the switch is now indicated in Telnet and WEB.<br>**Manager - Extensions:**<br>In the Device Editor the value for 'Total Reboots' is now indicated on the 'Global+Link State' tab.<br>The Device List is extended by the optional 'Total Boots' column. This column can be displayed, if required, via the 'Extra > Preferences > Device-List' menu. | | | ✓<br>**HW2** | ✓<br>**HW2** | | ✓<br>**HW2** | ✓ |
| [From V3.65am]<br>Local Logging implemented. With this function alarms are stored in the local log. In case of an internal memory overflow the oldest alarms will be deleted. The log can be displayed via WEB, Console and Manager.<br>**Manager - Extensions:**<br>In the Device-Editor the 'Local Logging' option was added to the 'Destination Type' parameter on the 'Alarm Destination Table' tab. Moreover, the local log can be displayed via the 'Show Local Log' button and the 'Show > Local Logging' menu. | | | ✓<br>**HW3** | ✓<br>**HW3** | | ✓<br>**HW3** | ✓ |
| [From V3.65am]<br>For management packets the IPv4 DSCP value was changed from 0 to 60. Thus it is possible to configure a unique IPv4 prioritisation of the management packets in the core switch. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65am]<br>For the Syslog message the Facility can now be configured in the range from 1 to 31. The set value applies to all alarm types.<br>**Manager - Extensions:**<br>In the Device Editor the 'Syslog Facility' parameter has been implemented on the 'Alarm Destinations' tab. | | | ✓ | ✓ | | ✓ | ✓ |
| [From V3.65ar]<br>Does only apply to switches using Mgmt hardware versions HW0 and HW1:<br>For Security firmware versions V3-SECURE/SNMP/TELNET and V3-GIGA/SEC/SNMP/TELNET the Simple Network Time Protocol (SNTP) is no longer supported. These are purely update versions for existing customers. | | | ✓ | | | | - |
| [From V3.65be]<br>Does only apply to the 'GigaSwitch V3' switch types:<br>Now for Port 5 (UPLINK-FO) the '1000 FDX (Autoneg. disabled' speed/duplex mode can be set. This mode is only required, if the Fiber Uplink is connected to an older unit (e. g. Fiber Converter).<br>**Manager - Extensions:**<br>In the Device Editor the 'Link Setup > Speed/Duplex' parameter on the Port tabs and the status display in the 'Link Setup' column on the 'Global+Link State' tab have been extended accordingly. | | | | ✓<br>**HW3** | | | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY | ENHANCED/ SECURITY | I-BASIC (1) | I-PROFES SIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| [From V3.65bx]<br>Now a Secure mode can be enabled for management access. If this mode is enabled, only secure protocols are accepted for access via CLI, WEB und SNMP. Moreover a secure password of a certain minimum complexity is enforced. If an insecure password is active when logging in via CLI or WEB, first a password change is enforced, before the switch can be configured.<br>With Industry switches this mode can be enforced using the DIP switch 3 (F1) on the rear, so that it cannot be disabled via management access.<br>**Manager - Extensions:**<br>In the Device Editor the 'Access Policy' parameter has been implemented on the 'Access Global' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | ✓ |
| [From V3.65da]<br>There is now the option to enable a password strength checker which presupposes a secure admin and user password.<br>Manager - Extensions:<br>On the Local Accounts tab the point's password strength checker and minimum password length were added. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | ✓ |
| [From V3.65dr]<br>With the command 'Disable if no link' the Admin State of a port can be set to 'Admin Disabled' depending of the current link state. This command will only be executed if no link is established.<br>It is especially for CLI scripts or master configurations and has the security advantage that all not connected ports are shut down. This setup will also take affect after a reboot.<br>**Manager – Extensions:**<br>In the Device-Editor the checkbox "Link Setup > Disable if no link (Self clearing after write)" was added to the Port tab. | | | ✓ | ✓ | | ✓ | ✓ |
| [From V3.65dr]<br>For ports that support PoE (Power over Ethernet) the PoE voltage can be disabled time controlled. To establish it the port must not been set to 'Off' and the time client must receive a valid time from the time server.<br>**Manager - Extensions:**<br>In the Device-Editor the parameter "Automatic Powersave" was extended with the configuration option "Set PoE Setup to 'Off' by Time Client". | | | ✓ | ✓ | | ✓ | ✓ |
| **Firmware - Portsecurity:** | | | | | | | |
| [From V3.65ar]<br>Ports, which were disabled via Portsecurity, now can optionally be re-enabled automatically after a settable period of time. The time value can be set in the range from 1 to 60000 seconds.<br>**Manager - Extensions:**<br>In the Device Editor the 'Re-Enable Time for Security-Disabled Ports' parameter has been implemented on the 'Security Setup' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | - |
| [From V3.65ar]<br>Ports, which were disabled via Loop-Protection, now can optionally be re-enabled automatically after a settable period of time. The time value can be set in the range from 1 to 60000 seconds.<br>**Manager - Extensions:**<br>In the Device Editor the 'Re-Enable Time for Loop-Disabled Ports' parameter has been implemented on the 'Security Setup' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | - |
| [From V3.65be]<br>Now the 'Unsecure-VLAN' setting for the 'Startup VLAN' can also be enabled when using IEEE802.1X. Previously this was possible for MAC-based security only. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65be]<br>On the WEB interface and CLI the memory card licence type is now shown under 'Device Info'. For enabling the Media Redundancy Protocol (MRP), e. g. a memory card with a corresponding MRP licence is required.<br>**Manager - Extensions:**<br>In the Device-Editor the 'Licence (optional)' display field has been implemented in the 'Memory Card Info' group on the 'Device Info' tab. | | | | | | ✓ **HW3** | ✓ |
| [From V3.65br]<br>The Portsecurity Renew command can now be executed on the CLI and WEB interface in the User Mode (Read/Only Access). Previously this was possible in Admin Mode (Read/Write Access) only. | | | ✓ | ✓ | | ✓ | - |
| **Firmware - Redundancy:** | | | | | | | |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY | ENHANCED/ SECURITY | I-BASIC (1) | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| [From V3.65ar]<br>Does only apply to 'E+' series Industry switches:<br>Zeroloss-Redundancy feature implemented. This feature allows to transmit e. g. IEC61850 GOOSE packets without loss in case of ring interruption.<br>**Manager - Extensions:**<br>In the Device Editor the new 'Redundancy > Zeroloss' tab has been implemented. | | | | | | ✓ **HW3** | ✓ |
| **Firmware - Command Line Interface (CLI):** | | | | | | | |
| [From V3.65ay]<br>Now a placeholder for the IP address or the name of the switch can be indicated with the TFTP CLI command for sending the config. The syntax is:<br>`# tf:tp <ip-address> p:ut <path> {<filename>.cfg\|$ip$.cfg\|$name$.cfg} [a:ll]` | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | - |
| [From V3.65ak]<br>With the 'show running-config' CLI command the SNMPv1/v2 communities, SNMPv3 passwords and RADIUS secrets can now be output in an encrypted form. The corresponding command is:<br>`config console-encryption enabled`<br>The encrypted values can then be used as input values for configuring the corresponding parameters.<br>**Manager - Extensions:**<br>In the Device-Editor the 'Encrypt passwords in CLI' parameter has been implemented in the 'Console Setup' group on the 'Access Global' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | ✓ |
| [From V3.65bv]<br>Does only apply to the 'GigaSwitch V3' switch types:<br>The socket below the label for the LED indicators can now be used as a local V.24 configuration interface. For this purpose a special V.24 configuration cable is required, which can be procured via Aginode.<br>**Manager - Extensions:**<br>In the Device-Editor the 'V.24 authentication mode' parameter has been implemented in the 'Console Setup' group on the 'Access Global' tab. | | | | ✓ **HW3** | | | ✓ |
| **Firmware - WEB:** | | | | | | | |
| | | | | | | | |
| **Firmware - SNMP:** | | | | | | | |
| [From V3.65am]<br>For SNMPv3 a third 'Flexible User' has been implemented, which can optionally be configured for 'Read/Write' or 'Read/Only'.<br>**Manager - Extensions:**<br>In the Device-Editor the 'SNMPv3 User Setup (Flexible)' group has been implemented on the 'Access SNMP' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | ✓ |
| [From V3.65am]<br>Privacy for SNMP Protocol Version 3 implemented. For encryption the same password as for authentication is used.<br>**Manager - Extensions:**<br>In the Device Editor the 'SNMP protocol version' parameter has been extended by the 'SNMPv3[Auth.-MD5][Priv.-DES]' and 'SNMPv3[Auth.-SHA][Priv.-DES]' options on the 'SNMP Access' tab. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | ✓ |
| [from V3.65aa]<br>Compatibility with several SNMPv3 management systems improved. Previously the SNMPv3 Discover process was occasionally aborted by Manager, because no zero values for 'msgAuthEngineTime' and 'msgAuthEngineBoots' were accepted by Manager. | | | ✓ **HW3** | ✓ **HW3** | | ✓ **HW3** | - |
| **Firmware – Bug Fixes:** | | | | | | | |
| [From V3.65aa]<br>Does only apply to switches using management hardware version HW3:<br>Enabling the 'VLAN Portmirror' function via Manager or CLI resulted in rebooting the switch. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65ab]<br>Does only apply to switches using management hardware version HW3:<br>If an IP multicast was received for an IP subnetwork, which was not part of the switch's subnetwork, an 'ICMP host not reachable' and 'ICMP port not reachable' message, respectively, was wrongly sent to the set gateway IP address. These ICMP messages are now prevented. | | | ✓ | ✓ | | ✓ | - |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB (1) | SNMP/ TELNET/ WEB (1) | SECURITY | ENHANCED/ SECURITY | I-BASIC (1) | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| [From V3.65ab]<br>Does only apply to switches using management hardware version HW3:<br>If no gateway was entered with the switch, under certain conditions ARP requests were transmitted using the source IP address of 0.0.0.0. This could lead to IP address conflicts with Windows PCs booting via DHCP. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65ac]<br>Does only apply to 'GigaSwitch V2+' and Desk or Industry switches with PoE adapter type 88301262 (here only PoE adapter hardware version 00):<br>From firmware version V3.64, although a PoE PD (consumer) was connected, power consumption per port was partly indicated as 0 Watt. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65ah]<br>Does only apply to switches from firmware version V3.61 supporting the Portmonitor feature:<br>If the VLAN-ID and the Trunking-Mode of the source and destination port were not set to identical values (with Portmonitor enabled), possibly not all packets of the source port were output on the destination port. Now the Active-VLAN-ID and the Active-Trunking-Mode of the Monitor destination ports are automatically set to the same values as the Monitor source port.<br>If this Portmonitor function was enabled via CLI, under certain conditions the 'renew' command had to be executed. Now this is not required any more. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65ah]<br>If the 'Manager authentication mode' and the 'SSHv2 authentication mode', respectively, were set to RADIUS, the 'Portsecurity realm' string was wrongly inserted in the user name of the RADIUS request. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65am]<br>With the 'Industrial Alarm M1' and 'Industrial Alarm M2' industrial alarm types partially wrong status texts were sent in SYSLOG messages. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65as]<br>If the Multiple Spanning Tree Protocol was enabled globally and the MSTP was disabled for some ports, these ports were wrongly permanently blocked after a power-up. | | | | ✓<br>**HW3** | | ✓<br>**HW3** | - |
| [From V3.65bg]<br>Does only apply to switches using management hardware version HW3:<br>In case of a high network load in the management VLAN an 'Internal Warning' alarm message was wrongly sent. | | | ✓<br>**HW3** | ✓<br>**HW3** | | ✓<br>**HW3** | - |
| [From V3.65bg]<br>This is only for "GigaSwitch V3", "GigasSwitch 54x Desk", "iGigaSwitch 54x" and "iSwitch 1043E+" with Mgmt Hardware Version 03:<br>While IGMP Snooping was activated and high multicast traffic was generated there was the possibility that the Switch was not accessible by management or that the switch reboots. | | | ✓<br>**HW3** | ✓<br>**HW3** | | ✓<br>**HW3** | - |
| [From V3.65bx]<br>There was the possibility by changing the VLAN setup via CLI (TELNET, SSH or V.24) and enter the "renew" command within two seconds that the VLAN setup was not assumed. | | | ✓ | ✓ | | ✓ | - |
| [From V3.65ck]<br>This is only for Switchtype 'GigaSwitch V3':<br>If a port had a RX Limiter for Flood-, Broadcast- and Multicast packets activated and this port was mirrored not all packets of the source port were send out trough the destination port. | | | | | | | |
| [From V3.65cn]<br>Does only apply to switches with management hardware version HW3 (except 'GigaSwitch V3'), which were delivered in May 2011 or later::<br>Under certain circumstances it could happen that the switches will reboot by itself. This was dependent on the type of network load in the management VLAN. | | | ✓<br>**HW3** | ✓<br>**HW3** | | ✓<br>**HW3** | - |
| [From 3.65dr]<br>While accessing the Management of the Switch with SNMPv2c or SNMPv3 get-bulk-request in combination with a high value for max-repetitions the SNMP get-response packet was formatted wrong | | | ✓ | ✓ | | ✓ | - |

## 2.13. Release V3.64

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Manager - Extensions:** | | | | | | | |
| Now Basic Configurator is an integral part of Manager and compatible with Windows Vista and Windows 7. A standalone installation of Basic Configurator is no longer supported. However, via a link in the Windows start menu (which is created during the installation or update of Manager) it is still possible to start Manager directly in the Basic Configurator mode. If the PC has several network interfaces, these will be scanned one after other in order to securely detect all switches on layer 2. | | | | | | | ✓ |
| The Device List was extended by a quick start bar. This bar allows you to run the most popular menu options with a click. | | | | | | | ✓ |
| In the Device List the 'Device List' and 'Configure' menu options and the right-click menu have been completely restructured and double entries removed. Many of the double entries now can more simply be run from the quick start bar. The import function for device lists was moved from the 'Device List' menu into the 'Add/Remove' menu and renamed to 'Add from Device-List ...'. | | | | | | | ✓ |
| Previously it was possible to assign different names for a device list and its file on the hard disk. Now only the file name is used as a name for the device list and displayed accordingly in the device list header. | | | | | | | ✓ |
| In the device list the 'Configure > Read CLI-Config of checked Devices' menu option has been implemented. This function allows you to read the CLI configurations of all selected switches. The configurations will automatically be saved in the Database directory under the name of xxx_xxx_xxx_xxx.cfg. | | | | | | | ✓ |
| In the Device Editor several tabs have been renamed to better reflect their function. | | | | | | | ✓ |
| In the Device Editor the 'Active Voice VLAN' is now displayed on the 'State > MAC+Security State' tab. Previously this was only indicated on the 'State > Global+Link State' tab. | | | | | | | ✓ |
| In the Device List and in the Device Editor the new 'Open WEB Browser (**HTTPS**) [Port xxx]' menu option has been implemented. The port number can now be set via the new 'WEB Browser HTTPS TCP Port' basic setting in the 'Extras > Preferences > Access' menu in the range of 1…65535. The default value is 443. Note: The port number must be identical in the switch and in Manager. | | | | | | | ✓ |
| In the Device List and in the Device Editor the 'Open WEB Browser' menu option has been changed to 'Open WEB Browser [Port xxx]'.<br>The port number xxx can be set (as before) via the 'WEB Browser TCP Port' basic setting in the 'Extras > Preferences > Access' menu in the range of 1…65535. The default value is 80. Note: The port number must be identical in the switch and in Manager. | | | | | | | ✓ |
| In the Device List and in the Device Editor the new 'Open SSH Client [xxxx.exe]' menu option has been implemented.<br>The SSH client application used is displayed in square brackets. This client application needs to be configured before in the new 'SSH Client' basic setting in the 'Extras > Preferences > Access' menu. | | | | | | | ✓ |
| In the Device List and in the Device Editor the 'Open Telnet Client' menu option has been changed to 'Open Telnet Client [xxx]'.<br>The Telnet client application used is displayed in square brackets. By factory default '[Windows default client]' is indicated, because the standard Windows client is started. However, this setting can be replaced via the 'Telnet Client' basic setting in the 'Extras > Preferences > Access' menu with any other client. | | | | | | | ✓ |
| During a firmware update the firmware image file size and the duration of the update are now indicated in the log file. The format is: <xxxxx bytes in xx secs> | | | | | | | ✓ |
| For industrial switches now the source of an alarm is indicated for each of the two alarm outputs M1 or M2 on the 'Global+Link State' tab. The display continues to be preserved, even if the alarm contact is disabled again. In this case the time period since the alarm has been disabled is additionally shown. The display of source and time can be deleted using the new 'Clear Alarms' button. | | | | | | | ✓ |
| On the 'Alarm Destination Table' a new button called 'Disable Destination' has been implemented for each of the eight destinations. By clicking on this button all settings in the corresponding column will be reset to their factory default. | | | | | | | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| If the 'Port Security Mode' is set to 'IEEE802.1X allow all MAC Addresses', 'IEEE802.1X Multi-User allow three MAC Addresses' or 'IEEE802.1X Client with MD5-Challenge' on the port tabs, now an information window is displayed informing about the special function of these modes. Here in any case the manual should be consulted before enabling any of these modes. This is because these modes make sense only for very specific security constellations. | | | | | | | ✓ |
| In Autodiscovery Layer-2 two new columns called 'Uptime' and 'Last seen' have been implemented in the list of detected switches. 'Last seen' shows the time of the last reception of an Autodiscovery response from the switch. | | | | | | | ✓ |
| The Device List was extended by a 'Serie/No.' column. This column shows the product series number and the current serial number of the switch. If required this column can be displayed via the Manager basic settings. | | | | | | | ✓ |
| The Device List was extended by the 'Device MAC Address' and 'MC MAC Address' columns. They show the MAC address of the switch or of the memory card. If required these columns can be displayed via the Manager basic settings. | | | | | | | ✓ |
| The Device List was extended by a 'Last seen' column. This column shows the date and time when the last polling response was received from the switch. If required this column can be displayed via the Manager basic settings.<br>Note: By default the columns 'Last seen' and 'Uptime' are not saved in the Device List file. If the Device List shall display the last values for these two columns after opening, the **Save columns 'Uptime' and 'Last seen' to Device-List** option is to be checked. | | | | | | | ✓ |
| In the Device List on the 'Redundancy > Spanning Tree' tab notes on finding the correct settings for the 'Max. age/hops', 'Hello time' and 'Edge port' parameters have been added. | | | | | | | ✓ |
| In the Device List in the 'Device-List' menu the new function 'Save as (checked Device only)' has been implemented. Contrary to the 'Save as' function, which saves all switches of the current device list under a new name, this new function only saves the selected switches. | | | | | | | ✓ |
| **Manager – Bug Fixes:** | | | | | | | |
| Under the 'Inventory > Create Excel Inventory-List …' menu the creation of the list was sometimes aborted because unexpected values were read from the database. Such values are now ignored and left empty in the inventory list. | | | | | | | ✓ |
| If very many switches are entered in the device list, the device freezes for several seconds, when the polling run starts or is running. Then the CPU load reaches almost 100% for the corresponding CPU core. This problem has been fixed. | | | | | | | ✓ |
| **Firmware – Basic Features:** | | | | | | | |
| Support for the 60 GigaSwitch V3 and 61 GigaSwitch V3 SFP switch types implemented. These switches have been designed in mosaic format and are equipped with on-board management principally supporting the complete set of functions of all firmware features. | | | | ✓ | | | ✓ |
| With switches of the GigaSwitch BM+ (from device hardware version 2) and GigaSwitch V2+ (from device hardware version 3) type, the gigabit TP ports now automatically switch into a Powersave mode, if no link is present. This saves about 0.4W of power per disabled port. | ✓ | ✓ | ✓ | ✓ | | | - |
| With switches with installed Power-over-Ethernet (PoE) option the available power, if any, is communicated to the terminal unit via CDP. This function is particularly relevant to Cisco access points with higher power consumption, since they do not boot correctly without the corresponding CDP information. The power requested via CDP by the terminal unit can be displayed using the 'Show Neighbor Details' function. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| New Speed/Duplex setting called 'ECO 10/100' for twisted-pair gigabit ports.<br>This setting is exclusively supported by gigabit ports in order to reduce power consumption. This makes sense, e. g. for terminal units which support a gigabit link, but for which a data rate of 100 Mbps is sufficient. Ports which are operated unnecessarily on a 1 Gbps link will need an additional power of about 0.5 Watt at the switch and at the terminal unit.<br>Note: Currently this function is supported for the 'GigaSwitch V3', 'GigaSwitch 541/542 Desk' and 'iGigaSwitch 541/542' switch types only.<br>**Manager - Extensions:**<br>In the Device Editor the 'Link Setup > Speed/Duplex' parameter on the port tabs and the status display in the 'Link Setup' column on the 'Global+Link State' tab have been extended accordingly. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| The new 'Overtemperature Powersave Action' feature allows you to configure an action which shall be triggered when the 'High Alarm Limit' temperature is exceeded.<br>Via the 'Set Speed/Duplex of ports with 'Autoneg.' or '1000FDX' to 'ECO 10/100' setting, ports supporting the 'ECO 10/100' Speed/Duplex mode will automatically be switched into this ECO mode in order to reduce power consumption.<br>Note: Currently this function is supported for the 'GigaSwitch V3', 'GigaSwitch 541/542 Desk' and 'iGigaSwitch 541/542' switch types only.<br>**Manager - Extensions:**<br>In the Device Editor the 'Overtemperature Powersave Action' parameter is implemented on the 'Alarms > Global Alarms' tab. | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ |
| The new 'Automatic Powersave' function allows you to automatically reduce the power consumption of the port.<br>The following setting is available:<br>Twisted pair ports supporting the 'ECO 10/100' Speed/Duplex mode can be switched time-controlled into this mode. As a precondition the Time Client must have received a valid time from the Time Server.<br>Time is controlled globally for all ports set accordingly. The times for each day of the week can be set separately via the Powersave setup of the Time Client.<br>Note: Currently this function is supported for the 'GigaSwitch V3', 'GigaSwitch 541/542 Desk' and 'iGigaSwitch 541/542' switch types.<br>**Manager - Extensions:**<br>In the Device Editor the 'Automatic Powersave' parameter is implemented on the port tabs and time-control can now be configured on the 'Time Client > Powersave Setup' tab. | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ |
| New VLAN Table mode designated as 'Static - 802.1Q based (64 VLANs)' implemented. This mode supports up to 64 static VLAN IDs from the range of 1… 4095.<br>Note: Currently this function is supported for all switch types having one or more gigabit ports.<br>**Manager - Extensions:**<br>In the Device Editor the 'VLAN Table Mode' parameter has been extended accordingly on the 'VLAN Table' tab. | ✓ HW2 | ✓ HW2 | ✓ HW2 | ✓ HW2 | ✓ | ✓ | ✓ |
| New VLAN Table mode designated as 'Static - Port based (16 VLANs)' implemented. All ports set to the same Default VLAN ID are transparently connected with one another. All packets (including a possibly present 802.1Q VLAN tag) will be transmitted without any change between these connected ports.<br>Note: Currently this function is supported for the 'GigaSwitch V3' and 'GigaSwitch 541/542 Desk' switch types and by all industrial switches.<br>**Manager - Extensions:**<br>In the Device Editor the 'VLAN Table Mode' parameter has been extended accordingly on the 'VLAN Table' tab. On the 'VLAN Setup' the 'Trunking Mode' parameter has been adapted. | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ |
| New function called 'Client Remove Alarm' implemented. This function detects, if a terminal unit has been permanently removed from the port. If the link of the monitored port is 'Down' for a configurable period of time (1…60000 seconds), a 'Client Remover Alarm' will be triggered which can be sent via the Alarm Destination Table.<br>**Manager - Extensions:**<br>In the Device Editor the 'Client Remove Alarm' and 'Link Down Timeout' have been implemented on the port tabs. On the 'Alarm Destinations' tab the 'Alarm Destination Table' has been extended with the 'Client Remove Alarm' alarm type. | | ✓ HW2 | ✓ HW2 | ✓ HW2 | ✓ | ✓ | ✓ |
| The 'Alarm Destination Table' has been extended by the 'Internal Management Warning' alarm type. This alarm type is sent in case of internal irregularities (e. g. available RAM memory too small, problems when accessing the switch engine, etc.). When receiving this warning the manufacturer's support service should be contacted.<br>**Manager - Extensions:**<br>In the Device Editor the 'Alarm Destination Table' has been extended by the 'Internal Management Warning' alarm type on the 'Alarm Destinations' tab. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| New option called 'Send Link Alarms' implemented. This option is enabled by default and ensures that the 'Link Up', 'Link Down' and 'Link Change' alarm types will be sent for the port concerned, provided they have also been enabled in the 'Alarm Destination Table'. If this option is disabled, no link alarms will be sent for the port concerned, not even, if these have been enabled in the 'Alarm Destination Table'.<br>**Manager - Extensions:**<br>In the Device Editor the 'Send Link Alarms' parameter has been implemented on the port tabs. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| The new 'VLAN Port Isolation' function can now be used to principally isolate all user ports from one another. This applies in particular for ports assigned to the same VLAN. In this case, user ports can exchange data with uplink ports only.<br>Note: Currently this function is supported for the 'GigaSwitch V3' and 'GigaSwitch 541/542 Desk' switch types and by all industrial switches.<br>**Manager - Extensions:**<br>In the Device Editor the 'VLAN Port Isolation' parameter has been implemented on the 'VLAN Table' tab. | | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ |
| New parameter called 'IGMP Immediate Leave Mode' implemented. This parameter defines the treatment of 'IGMP Immediate Leave Messages'. By sending this IGMP message a connected terminal unit may request its immediate leaving of a multicast group<br>The following settings are possible:<br>• Accept Leave messages from User Ports only<br>• Accept all Leave messages<br>• Ignore all Leave messages<br>**Manager - Extensions:**<br>In the Device Editor the 'IGMP Immediate Leave Mode' parameter has been implemented on the 'IGMP Multicast' tab. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Industrial switches provide two outputs designated as M1 and M2. For the configuration of these outputs three new modes have been implemented:<br>• Function Input from Remote Switch:<br>With this setting the alarm output is controlled depending on the functional input of another Aginode industrial switch.<br>• Alarm Destination from Remote Switch:<br>With this setting the alarm output is controlled depending on the 'Alarm Destination Table' of another Aginode switch (may also be an Office switch).<br>• Alarm Destination from Local Switch:<br>In this case the alarm output is controlled depending on its own 'Alarm Destination Table'.<br>**Manager - Extensions:**<br>In the Device Editor the 'Alarm Output M1' and 'Alarm Output M1' parameters have been extended accordingly on the 'Industrial Alarms' tab. Furthermore the 'Remote Alarm Group M1' and 'Remote Alarm Group M1' parameters have been implemented. | | | | | ✓ | ✓ | ✓ |
| Industrial switches of the S, E and E+ Series have a functional input designated as 'Func.'.<br>This functional input can now be used to switch the alarm outputs M1 and M2 of a remote switch. This function is configured via the 'Remote Alarm Mode' and requires another Aginode industrial switch installed on the opposite side.<br>**Manager - Extensions:**<br>In the Device Editor the 'Remote Alarm Mode' and 'Remote Alarm Group' parameters have been implemented on the 'Industrial Alarms' tab. | | | | | ✓ | ✓ | ✓ |
| The 'Bandwidth Limiter' has been extended by the 'Limit all Packet Types (TCP/IP burst compatible)' packet type. This setting allows the RX-Limiter to shape the traffic of bursty TCP/IP data streams. For optimum function this procedure requires the 'Flow Control State' to be enabled on the corresponding port.<br>Note: Currently this function is supported for the 'GigaSwitch V3', 'GigaSwitch 541/542 Desk' and 'iGigaSwitch 54x' switch types.<br>**Manager - Extensions:**<br>In the Device Editor the 'Bandwidth Limiter - Packet Type' parameter has been extended accordingly on the port tabs. | | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ |
| DHCP Relay Agent (Option 82) feature implemented.<br>Note: This mode of function is not yet documented in the Manual. For detailed configuration information please contact Aginode Support.<br>**Manager - Extensions:**<br>In the Device Editor the new 'DHCP Relay Agent' tab has been implemented. | | | | ✓ **HW3** | | ✓ **HW3** | ✓ |
| For the authentication of name/password for Telnet, SSHv2, V24 and Manager login separate RADIUS settings can now be configured.<br>**Manager - Extensions:**<br>In the Device Editor the new 'RADIUS Management Authentication' tab has been implemented. Furthermore the 'MAC+Security State' tab has been extended by the 'Mgmt Authentication Server 1' and 'Mgmt Authentication Server 1' status display for Management RADIUS Servers. | | | ✓ **HW2** | ✓ **HW2** | | ✓ **HW2** | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| Support for PSE+ according to IEEE802.3at implemented. The connected terminal unit can be provided with a power of up to 30W.<br>Via the 'Auto 802.3at High-Power' mode terminal units also supporting the IEEE802.3at standard can be supplied with up to 30W.<br>Via the 'Auto 802.3af High-Power (Ignores Powerclass)' terminal units, which support the old IEEE802.3af standard, but require more power than 15.4W, can also be supplied with up to 30W.<br>Note: Currently this function is supported for the 'GigaSwitch V3 TP (PSE+)' switch type only.<br>**Manager - Extensions:**<br>In the Device Editor the 'PoE Setup' parameter has been extended accordingly on the port tabs. | | | | ✓ **HW3** | | | ✓ |
| Support for Cisco access points with higher power consumption implemented. These access points do not negotiate the required power via the new IEEE802.3at standard but via CDP and the Cisco 'Intelligent Power Management'. If such an access point is to be operated on a Aginode PoE port, CDP must additionally be enabled in the Aginode switch. Then the switch will send the required information via CDP to the access point.<br>**Manager - Extensions:**<br>In the Device Editor the display of the power characteristics requested by the access point has been added on the port tabs when selecting the 'Show Neighbour Details' button. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The green port LEDs of the 'GigaSwitch BM' and 'GigaSwitch V2+' switch types can be configured via Management. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| For the green port LEDs a new display mode called 'Show Link/Speed-Duplex' has been implemented. This mode facilitates the combined display of Link, Speed and Duplex. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Manager access via UDP and TFTP can now be completely disabled. This setting can only be configured via the 'config manager-auth-mode disable' CLI command. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Firmware - Portsecurity:** | | | | | | | |
| The 'IEEE802.1X Multi-User allows three MAC Addresses' Portsecurity mode function has been extended:<br>The port will be switched into the Unsecure VLAN as long as no client is authenticated.<br>If a default VLAN is configured (VLAN-ID = 1…4095), after successful authentication of at least one client, the port will always be switched to the configured default VLAN.<br>If no default VLAN is configured (VLAN-ID = 0), the switch expects the VLAN ID to be assigned by the RADIUS server. Here the first received VLAN-ID transmitted for a successfully authenticated (via IEEE802.1X or MAC-Bypass) client by the RADIUS server, is used.<br>Via these functions PCs and other devices may be authenticated, on which, in addition to their own MAC address, further MAC addresses of virtual machines are used.<br>Additionally, clients can be automatically removed from the port's MAC list after a selectable period of time via the Portsecurity Address Ageing function. This makes sense, if another switch follows after the switch port, so that a link-down of the client cannot be detected.<br>**Manager - Extensions:**<br>In the Device Editor on the 'Security > Security Setup' tab the 'Ageing time (minutes)' parameter has been complemented by the note on 'IEEE802.1X Multi-User…'. | | | ✓ | ✓ | | ✓ | ✓ |
| New 'Toggle Link' function implemented.<br>If this function is enabled, after a successful RADIUS MAC authentication (e. g. via IEEE802.1X MAC Bypass) the link of the corresponding port is interrupted for one second. This forces the connected terminal unit to request a new IP address via DHCP. The already learned MAC addresses of the switch port are preserved.<br>This function is useful, if the terminal unit has first received an IP address in the Unsecure-VLAN and shall be moved to another VLAN with a different IP range after successful MAC authentication.<br>**Manager - Extensions:**<br>In the Device Editor the new 'Toggle Link' parameter has been implemented on the port tabs. | | | ✓ | ✓ | | ✓ | ✓ |
| Here you can now define, whether IEEE802.1X EAP packets which receive the MAC address of a phone in the voice VLAN as a destination address, will be transmitted with or without a tag. The correct setting depends on the specification made by the corresponding phone manufacturer.<br>**Manager - Extensions:**<br>In the Device Editor the new 'EAP packets within Voice-VLAN' parameter has been implemented on the 'Security > IEEE802.1X' tab. | | | ✓ | ✓ | | ✓ | ✓ |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| For the RADIUS MAC Bypass the new 'Send single MAC-based RADIUS request' mode has been implemented. If, with this setting, the MAC address is rejected by the RADIUS server, then only authentication attempts according to IEEE802.1X will be performed. If an authentication of the MAC address shall be triggered again, this can be done via a short 'Link-Down' or the 'Renew' command.<br>**Manager - Extensions:**<br>In the Device Editor the 'RADIUS MAC Bypass' parameter has been extended accordingly on the 'Security > IEEE802.1X' tab. | | | ✓ | ✓ | | ✓ | ✓ |
| If IEEE802.1X 'Re-Authentication' is enabled, a re-authentication of the MAC address is performed in case of an IEEE802.1X 'RADIUS MAC Bypass'. The re-authentication interval for the MAC address corresponds to the IEEE802.1X 'Re-Authentication interval'. | | | ✓ | ✓ | | ✓ | - |
| **Firmware - Redundancy:** | | | | | | | |
| Multiple Spanning Tree protocol according to IEEE802.1Q implemented.<br>Up to eight MSTI instances are supported.<br>Note: Currently this function is supported for the 'GigaSwitch V3', 'GigaSwitch 541/542 Desk' switch types and all industrial switches.<br>**Manager - Extensions:**<br>In the Device Editor the 'Multiple Spanning Tree (MSTP)' setting can now be selected for the 'Protocol Version' parameter on the 'Redundancy > Spanning Tree' tab. Moreover the new 'Redundancy > Multiple Spanning Tree' tab for configuring the MSTP instances has been implemented. | | | | ✓ **HW3** | | ✓ **HW3** | ✓ |
| The 'Max. age' Spanning Tree parameter has been renamed to 'Max. age/hops' and the configurable maximum value increased from 40 to 50. Thus up to 50 switches can now be switched in a ring.<br>**Manager - Extensions:**<br>Notes in the maximum parameter values have been added to the 'Max. age/hops' and 'Hello time' parameters. | | | | ✓ | | ✓ | ✓ |
| DHCP Relay Agent (Option 82) feature implemented.<br>Note: This mode of function is not yet documented in the Manual. For detailed configuration information please contact Aginode Support.<br>**Manager - Extensions:**<br>In the Device Editor the new 'DHCP Relay Agent' tab has been implemented. | | | | ✓ **HW3** | | ✓ **HW3** | ✓ |
| Media Redundancy Protocol (MRP) on the basis of IEC 62439-2 implemented.<br>Note: This mode of function is not yet documented in the Manual. For detailed configuration information please contact Aginode Support.<br>**Manager - Extensions:**<br>In the Device Editor the new 'MRP' tab has been implemented. | | | | | | ✓ **HW3** | ✓ |
| **Firmware - Command Line Interface (CLI):** | | | | | | | |
| The 'show run' CLI command can now be called using the `no-pause` option, in order to return the configuration in one go.<br>The general syntax is:<br>`sh:ow ru:nning-config [a:ll] [n:o-pause]`<br>This option is primarily intended for CLI scripting for archiving the configuration. | | ✓ **HW2** | ✓ **HW2** | ✓ | ✓ | ✓ | - |
| When the user enters the wrong name or password three times, all console interfaces (SSH, TELNET and V.24) will be locked for 60 seconds. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| When logging in using the CLI console (Telnet, SSH and/or V2.24) now information on the mode of function of the 'help' CLI commands is automatically displayed. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| **Firmware - WEB:** | | | | | | | |
| HTTPS implemented. Independent of the HTTP supported in parallel, a separate authentication mode and TCP port can be configured here.<br>**Manager - Extensions:**<br>In the Device Editor the new 'HTTPS Authentication Mode' and 'HTTPS TCP Port' parameters have been implemented on the 'Management > Access Global' tab. | | | | ✓ **HW3** | | ✓ **HW3** | ✓ |
| The 'autocomplete='off'' HTTP code now prevents the WEB browser from saving the switch's passwords. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| When the user enters the wrong name or password three times, all WEB interfaces (HTTP and HTTPS) will be locked for 60 seconds. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| **Firmware - SNMP:** | | | | | | | |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| New version of the Aginode Switch MIB: NEX-BM.MIB Version 3.94. The following changes/extensions have been implemented:<br>- bmSwitchInfo: object infoAlarmStateM1/infoAlarmStateM2: enum alarmOnRemoteFunctionInput(12), alarmOnRemoteAlarmDestTable(13) and alarmOnLocalAlarmDestTable(14) added<br>- bmSwitchInfo: object infoLastInternalMgmtWarning added<br>- bmSwitchAdmin: object adminSwitchVlanTableMode: enum staticModeVlans64(3) added<br>- bmSwitchAdmin: object adminSwitchVlanTableMode: enum staticModePortBased(4) added<br>- bmSwitchAdmin: object adminAlarmM1 and adminAlarmM2 added<br>- bmSwitchPortTable: object portSpeedDuplexSetup: enum afHighPower(7) and atHighPower(8) added<br>- bmSwitchPortTable: object portPoeAdminState: enum eco(9), ecoOverTemp(10) and ecoPowerSave(11) added<br>- bmSwitchPortTable: object portLEDGreen: enum showLinkSpeedDuplex added<br>- bmSwitchPortTable: object portLimiterPacketType: enum limitAllPacketsBurstsAllowed added<br>- trap clientRemoved added<br>- trap internalMgmtWarning added | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| New 'SNMP protocol version' function implemented. This allows you to define the SNMP protocols used to access the SNMP-MIB of the switches.<br>**Manager - Extensions:**<br>In the Device Editor the new 'SNMP protocol version' parameter has been implemented on the 'SNMP Access' tab. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SNMP Protocol Version 2c implemented. The 'SNMP protocol version' parameter can be used to define whether access via SNMPv2 is allowed.<br>**Manager - Extensions:**<br>In the Device Editor the 'SNMP protocol version' parameter has been extended by the 'SNMPv2c' and 'SNMPv1 and SNMPv2c' options on the 'SNMP Access' tab. | | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ **HW2** | ✓ |
| SNMP Protocol Version 3 implemented. The 'SNMP protocol version' parameter can be used to define whether access via SNMPv3 is allowed. For authentication the Username and MD5 and SHA Password Hash, respectively, of the packet are analysed and checked. No encryption of the data is performed.<br>**Manager - Extensions:**<br>In the Device Editor the 'SNMP protocol version' parameter has been extended by the 'SNMPv3[Auth.-MD5][No Priv.]:' and 'SNMPv3[Auth.-SHA][No Priv.]:' options on the 'SNMP Access' tab. Moreover, parameters for configuring the SNMPv3 user names and password have been implemented on this tab. | | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ **HW3** | ✓ |
| For SNMPv1 and SNMPv2c now a separate Trap Community can be configured. If this is empty, the Read/Only Community will be used for sending SNMP traps.<br>**Manager - Extensions:**<br>In the Device Editor the new 'Trap community' parameter has been implemented on the 'SNMP Access' tab. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| New version of the global Aginode MIB: AGINODE.MIB Version 3.8. The following changes/extensions have been implemented:<br>- bmSwitch: products {bmSwitch 60,61} added | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| With industrial switches the two alarm outputs M1 or M2 can now be configured via SNMP. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| **Firmware – Bug Fixes:** | | | | | | | |
| After an uptime of '49 days : 17 hours : 2min' (or multiples thereof) several functions of the switch were frozen at a probability of 1:20 to 1:100. This included e. g. an update of the uptime and link-up detection. But, as long as no link-down occurred on such a switch, the switch continued to operate without any restriction. Whether or not a switch is in the above mentioned state can be seen in the 'Uptime' frozen. This problem occurs at a higher probability with switches with enabled Spanning Tree (about 1:20). Here an update should be made to the current release shortly. | | | | ✓ | | ✓ | - |
| Under certain conditions IEEE802.1X EAP success packets were wrongly sent with VLAN tag, if a new VLAN had previously been assigned via RADIUS server. | | | ✓ | ✓ | | ✓ | - |
| In the Info on the PoE adapter in WEB ('Info' page) and in the TELNET/SSH/V.24 console (show info) a six-digit 'Production number' was wrongly indicated as '0000'. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| After switching the IGMP on or off, a reboot had to be performed. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| In case of a very high IGMP multicast traffic it was possible that the switch management could not be accessed any longer. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |

| Switch family➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| **Firmware family ➔** | **WEB** | **SNMP/ TELNET/ WEB** | **SECURITY** | **ENHANCED/ SECURITY** | **I-BASIC** | **I-PROFESSIONAL** | **NexManV3 Switch Manager** |
| **Bundle code ➔** | **-** | **-** | **-** | **ES3** | **-** | **PRO2 PRO3** | **-** |
| The wrong time was handed over with the SNMP variable of 'ifLastChange'. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| The 'bmSwitchInfoNoOfReboots' SNMP counter was wrongly indicated as an INTEGER type. This was corrected to the COUNTER-32 type. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Applies only to switches with HW0, HW1 or HW2 management hardware version: With certain settings of the TCP/IP Stacks in PC, HTTP access could be blocked when accessing the HTTP interface. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| With certain switch types the remote fault function on the uplink port was enabled immediately after rebooting, although it was actually disabled via Management. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| With SNMP traps the port-related variables were partly sent without the 'if-index'. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Does only apply to switches with firmware version V3.61 to V3.62kx and management hardware versions HW0, HW1 or HW2:<br>If the switch was started with the 'Reboot to Factory-Default' function (via reset plug, DIP switch 2 or Management command), with the next normal reboot with Flash configuration a portion of the configuration was again reset to factory default. That means, after a factory default reboot first a second normal reboot had to be performed, before effective changes to the configuration could be realised. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Does only apply to switches with firmware version V3.61 to V3.62hc and management hardware versions HW0, HW1 or HW2:<br>The switch did not react after some time, if unauthorised TFTP accesses to the switch had been performed. This might be caused e. g. by security network scanners checking all network devices for open ports. These possibly try to regularly read a file via TFTP, but are not authorised to do so and are rejected. Each of these unauthorised TFTP accesses caused an additional memory leak until the complete RAM memory of the Management module was used up and access to the switch was blocked. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Relevant only to industrial switches with management hardware version HW2:<br>If, upon booting the switch, it is determined that the firmware is corrupt, now automatically a switchover to the fixed IP address 172.23.44.111 is performed.<br>This is particularly useful for industrial switches with HW2 management hardware. Here the front panel 'Set' push-button does not function, if the firmware is corrupt. So the switch would have to be opened in order to access the management module's switches. A corrupt firmware condition is signalled by a nonluminous green Mgmt LED. In this case now the fixed IP address will be enabled and a new update can be performed via this address. | | | | | ✓ | ✓ | - |
| On the console, when entering the 'show running-config' and 'show configuration interfaces' commands, respectively, the configuration setting for 'Remote Fault enable' was not shown. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Relevant only to switches with HW0, HW1 or HW2 management hardware version:<br>When entering the 'Test Traps/Syslog' command the SNMP traps were partly sent without files attached. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Relevant only to switches with HW2 management hardware version:<br>Accessing the LLDP-MIB via SNMP Get-Request results in a switch reboot. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Does only apply to switch types 'GigaSwitch 541/542 Desk' and 'iGigaSwitch 541/542':<br>Executing cable diagnostic for a single port will result in wrong cable length for all port with no cable connected. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |

## 2.14. Release V3.61

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| EVALUATION VERSION: Without valid license key the Manager will run in Evaluation mode only. Now up to five switches can be saved to a Device List and reloaded. Before it had not been possible to save or reload a Device List. Now a more realistic test of the Manager with test settings is possible. | | | | | | | ✓ |
| SECURITY: A new parameter "SSHv2 Authentication Mode" has been implemented on the "Management -> Access Global" tab. This function requires management hardware version 3 and a suitable security firmware version. | | | | | | | ✓ |
| DEVICE-LIST: New function under menu "Configure > Open Device-Editor by IP Address" implemented. Here it is possible to start the Device-Editor for a Device by directly entering the corresponding IP address. It is not necessary that the device is listed in the Device-List. | | | | | | | ✓ |
| SECURITY: Two new parameters has been implemented on the "VLAN -> VLAN Setup" tab:<br>- RADIUS Guest VLAN-ID (may be activated if the RADIUS server rejects the authentication)<br>- RADIUS Inaccessible VLAN-ID (may be activated if all RADIUS Server are down)<br>For a detailed explanation consult the new flowcharts within the firmware manual. | | | | | | | ✓ |
| SECURITY: Auf den Reitern "State -> Global+Link State" und „State -> MAC+Security State" wird nun jeweils in der Spalte „Security State" der Text "RADIUS Server(s) down" angezeigt falls alle konfigurierten RADIUS Server auf einen RADIUS Request für den betreffenden Port nicht antworten. | | | | | | | ✓ |
| SECURITY: The columns „Active Default VLAN-ID" on the "State -> Global+Link State" and „State -> MAC+Security State" tabs will now show the source of the active VLAN-ID (Unsecure VLAN, Guest VLAN, Inaccessible VLAN, IEEE802.1X Authentication Failure VLAN, Port Default VLAN, RADIUS VLAN).<br>Note: This setting is relevant to ports with activated Portsecurity Mode with authentication via RADIUS server only (IEEE802.1X or MAC-based). | | | | | | | ✓ |
| DEVICE-EDITOR: The CLI configuration of the switch can now be read, saved and indicated via the "Config" menu. Here three menu items are available:<br>- Read CLI Config (only with parameters changed from Factory-Defaut)<br>- Read CLI Config (with all parameters)<br>- Show CLI Config<br>The first menu item corresponds to the "show running-config" Telnet command and the second menu item to the "show running-config all" command. After reading the configuration is automatically saved in the Database directory under the name of xxx_xxx_xxx_xxx.cfg and displayed. When the configuration is saved, the Manager automatically inserts a comment header with date and time.<br>The "Show CLI Config" menu command can be used to display a saved configuration.<br>Note: This function is available only for switches with management hardware version 2 or higher and appropriate firmware. Otherwise the above menu items are deactivated | | | | | | | ✓ |
| DEVICE_LIST: If the Manager is started with an empty Device List (typically after initial installation) a pop-up window now first asks if an Autodiscovery LAYER-2 shall be started directly. | | | | | | | |
| DEVICE_LIST: The combination of Shift + left click allows you to select ranges in the Device List. When you subsequently right click in this selection all check marks can be set or removed. | | | | | | | ✓ |
| DEVICE_LIST: The waiting time is immediately cancelled for the firmware update, when the "Cancel Button" is pressed during the "Rebooting Device" log message. | | | | | | | ✓ |
| DEVICE_LIST: With computers with VISTA operating system the "Ping only" status is now correctly displayed. This is the case, e. g. if an unknown device was added to the Device List. This device answers to Ping requests only and not to the Manager's UDP status requests. Previously VISTA blocked Ping requests from the Manager. | | | | | | | ✓ |
| DEVICE/MASTER-EDITOR: In the "Templates" menu of the Device Editor a new function called "Update existing Master-Configs with new Firmware features of this Device" was implemented. A firmware update mostly adds new configuration settings of the switch, which then are immediately activated in the Device Editor of the current Manager. However, these new functions are not immediately available with existing Master | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| Configs, which were derived from an older firmware version. The problem is that the Manager activates only those functions which are supported by the respective 'old' firmware. With the new menu function the scope of functions of a new firmware can be transferred to any number of Master Configs. All configuration settings in the Master are retained, only the new configuration parameters will be set to their Factory Default values. Note: All switches in the network should receive the new firmware before executing this update function. | | | | | | | |
| DEVICE-EDITOR: A new column called "Syslog Severity" was implemented on the "Alarms -> Alarm Destinations" tab. This column can be used to set for each type of alarm with which Syslog Severity it shall be sent. Note: This setting is only relevant to destinations, for which the "Remote Syslog" Destination Type was selected. | | | | | | | ✓ |
| MASTER-EDITOR: Here the switch names and locations can be assigned via CSV file. For this purpose an external CSV file to be searched for the MAC address of the respective switch can be selected on the "Management -> Agent" tab. You can choose among the following CSV formats:<br>- Get Name from CSV file by MAC Address (xx:xx:xx:xx:xx:xx;name)<br>- Get Name from CSV file by MAC Address (xxxxxxxxxxxx;name)<br>- Get Name and Location from CSV file by MAC Address (xx:xx:xx:xx:xx:xx;name;location)<br>- Get Name and Location from CSV file by MAC Address (xxxxxxxxxxxx;name;location)<br>When the MAC address is found, the indicated name/name and location is accepted. Additionally the log book shows, if and which name/location was inserted. Note: Possible letters in the MAC address are accepted as upper and lower case. | | | | | | | ✓ |
| DEVICE-EDITOR: Three new parameters for the PoE (Power-over-Ethernet) input voltage have been implemented on the "Alarms -> Global Alarms" tab:<br>- "PoE Input Power Limit (VA)": This parameter was moved from the "Global" tab to this new place.<br>- "PoE Input Voltage Low Alarm Limit" and "PoE Input Voltage Upper Alarm Limit": Here the limit values for the PoE input voltage can be configured. An appropriate SNMP trap and a SYLOG message are sent only after violation of the "Low Alarm Limit" and "Upper Alarm Limit" respectively. With switches with installed PoE option, but without installed PoE input voltage (for later retrofitting with a PoE adapter), it is possible to inhibit alarms by setting the "Low Alarm Limit" to the value of 0. | | | | | | | ✓ |
| DEVICE-LIST: New "PoE" column implemented. The "Powered" text shows that a PoE option is installed in the switch and that the switch is supplied with the required 48V input voltage. If there is no 48V input voltage available (only possible for switches with separate power supply for switch and PoE), the text "Not Powered" will be displayed. If the "PoE Input Voltage Low Alarm Limit" is set to a value above 0 Volt, an alarm will be indicated in the "Alarms" column. If no PoE option is installed in the switch, "n/a" (not available) will be displayed.<br>IMPORTANT NOTE: If you are updating an already installed Manager, the new "PoE" column is not visible at first. However, you can activate it via the menu "Extra -> Preferences -> Device-List". | | | | | | | ✓ |
| DEVICE-LIST: New Inventory function implemented under the "Inventory -> Create CSV MAC-Address-List for Master-Config from Database (xx:xx:xx:xx:xx:xx;Device-Name)" menu item. Here you can create a CSV file on the basis of the installed devices, which contains the MAC addresses and the names of all devices (format = xx:xx:xx:xx:xx:xx;Device Name). This list can then be edited manually and be used as input for a Master-Config later in order to update the device names. | | | | | | | ✓ |
| DEVICE-LIST: Two new columns "Def. VLAN" and "Voice VLAN" implemented. The Default VLANs and the Voice-VLANs configured on the ports are indicated here. The individual VLAN-IDs are listed separated by commas with double IDs being listed only once.<br>IMPORTANT NOTE: After a new installation or an update the two columns are not visible. However, you can activate them via the menu "Extra -> Preferences -> Device-List". | | | | | | | ✓ |
| DEVICE-LIST: New column "Uptime" implemented. Here the operating time of the switch since the last reboot is indicated.<br>IMPORTANT NOTE: After a new installation or an update this column is not visible. However, you can activate it via the menu "Extra -> Preferences -> Device-List". | | | | | | | ✓ |
| DEVICE-EDITOR: In the table "Port Link State" a new column called "Power Setup" was implemented on the "Global+Link State" tab. Here the PoE setting for the respective port is indicated. Note: This column is shown only for devices with | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| installed PoE option. | | | | | | | |
| DEVICE-EDITOR: In addition to Name/Location/Contact, the configuration of a domain name is also possible on the "Agent" tab. | | | | | | | ✓ |
| DEVICE-LIST: In the "MAC Address " column now the addition ":MMC" shows whether the indicated MAC address comes from an installed MMC card. Note: MMC cards for saving the configuration are exclusively supported by industrial switches. For the MAC address of the MMC card to be taken over as the active MAC address of the switch, the MMC card must be installed when the switch is booted. | | | | | | | ✓ |
| DEVICE-LIST: In the "Alarms" column devices which respond to a Ping only are additionally marked with the "Ping only" text (previously they had only been marked with a light green field in the "Check" column). When the Device List is sorted by the "Alarms" column these devices will now be moved to the beginning of the Device List. When the mouse pointer is moved across a red field in the "Check" or "Alarms" columns, a help text is indicated giving further explanations. | | | | | | | ✓ |
| DEVICE-LIST/-EDITOR: The timeout interval for a device in the Device List or in the Device Editor to be indicated as Offline can now be configured under "Extras –> Preferences -> Global -> Timeout for status requests (seconds) ". An extension might be necessary, if there is a slow modem dial-in connection or similar between management PC and the monitored switches. | | | | | | | ✓ |
| DEVICE-EDITOR: The "Exit" command was split up into the "Exit & Save" and "Quit" commands. Both commands now do without the former conformation prompt whether the changed configuration shall be saved. With "Exit & Save" the configuration is automatically saved, if it was changed or newly read by the device. With "Quit" the Device Editor is closed without saving the configuration. Note: The former "Exit" function continues to be available by clicking the "X" in the upper right corner of the window. | | | | | | | ✓ |
| SECURITY: New "Voice VLAN Authentication Mode" parameter implemented on the "Security -> Security Setup" tab. This parameter is used to configure whether authentication according to IEEE802.1X or MAC-based shall be deactivated (bypass function) for devices whose MAC addresses are detected in the Voice VLAN (IP-Phones). Note: This setting is relevant to ports with activated Portsecurity Mode with authentication via RADIUS server (IEEE802.1X or MAC-based). The default setting is "Enable Authentication". | | | | | | | ✓ |
| SECURITY: The "PORT ERROR DISABLED" Security State was split up into "SECURITY DISABLED" and "LOOP DISABLED" depending on the indicated error status. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| INVENTORY: When executing the function "Inventory -> Create Excel Inventory-List for checked Devices from Database" under certain circumstances the Manager could crash. | | | | | | | ✓ |
| DEVICE-EDITOR: The Cable Diagnostic button was wrongly activated on the "Port Setup -> Port 0 [Mgmt]" tab. | | | | | | | ✓ |
| MASTER-EDITOR: The "Show SFP Info" button was wrongly activated on the "Alarms -> SFP Alarms" tab. This applied only to switches with SFP slots und support of the SFP diagnostic function. | | | | | | | ✓ |
| DEVICE-EDITOR: When a new VLAN-ID was added via the "Add" button on the "VLAN -> VLAN Table" tab, a new text entered previously in the "VLAN-Name" column was deleted. | | | | | | | ✓ |
| DEVICE-EDITOR: Under certain circumstances (mostly with a high CPU load of the PC) the Manager crashed displaying the error message 'Error during the creation of a windows handle'. | | | | | | | ✓ |
| DEVICE-EDITOR: Under certain circumstances it could happen that a firmware update was indicated as failed, although it was correctly completed. | | | | | | | ✓ |
| DEVICE-EDITOR: Under certain circumstances it could happen that the "Port Link State" scrolling bars on the "Global+Link State" tab were missing. | | | | | | | ✓ |
| FIRMWARE UPDATE: After a firmware update of switches installed in a Rapid Spanning Tree ring, sometimes it was wrongly indicated that the update failed. This problem was fixed. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| BASIC FUNCTION: Support implemented for management hardware version HW3. Note: Separate firmware versions are available. | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 | ✓ HW3 |
| BASIC FUNCTION: Support implemented for switch type 27 'GigaSwitch 541 Desk'. This desk switch has four 10/100/1000Mbps twisted pair ports and one 1000Mbps fiber | ✓ | ✓ | ✓ | ✓ | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| port. | | | | | | | |
| BASIC FUNCTION: Support implemented for switch type 28 'GigaSwitch 542 SFP Desk'. This desk switch has four 10/100/1000Mbps twisted pair ports and two 100/1000Mbps SFP VARIO slots. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| BASIC FUNCTION: Support implemented for 'Option PoE Type af 4-15 B 31W'. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| BASIC FUNCTION: Support implemented for switch type 36 'iSwitch 1043 3VI'. Unlike the ' iSwitch 1043' this switch has three 100/1000Mbps SFP VARIO slots. | | | | | ✓ | ✓ | ✓ |
| BASIC FUNCTION: Support implemented for switch type 37 'iGigaSwitch 541'. This industrial switch has four 10/100/1000Mbps twisted pair ports and one 1000Mbps fiber port. | | | | | ✓ | ✓ | ✓ |
| BASIC FUNCTION: Support implemented for switch type 38 'iGigaSwitch 542 SFP-2VI'. This industrial switch has four 10/100/1000Mbps twisted pair ports and two 100/1000Mbps SFP VARIO slots. | | | | | ✓ | ✓ | ✓ |
| BASIC FUNCTION: Support implemented for 'iOption PoE Type af 4-15 B'. | | | | | ✓ | ✓ | ✓ |
| ISWITCH: The response time of the Set pushbutton till the lightening up of the Set LED was shortened from five to three seconds. | | | | | ✓ | ✓ | - |
| PoE: Now it is possible to configure the limit values for an alarm message for the PoE (Power-over-Ethernet) input voltage. An appropriate SNMP trap and a SYLOG message are sent only after violation of the "Low Alarm Limit" and "Upper Alarm Limit" respectively. With switches with installed PoE option, but without installed PoE input voltage (for later retrofitting with a PoE adapter), it is possible to inhibit alarms by setting the "Low Alarm Limit" to the value of 0. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| PoE: If the PoE voltage on a port was switched off due to a PoE Overload Error, this error is now reported to the Manager and indicated there in the "Alarms" column of the device list. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LLDP: If an IPv4 address is sent as chassis-ID, this will now be shown under "Neighbor Details" also in the usual IP notation (X.X.X.X). In addition, MAC addresses will be returned in the corresponding hexadecimal notation (xx:xx:xx:xx:xx:xx) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SECURITY: The "Allowed MACs Overflow Address" now continues to be shown also after the respective port has automatically been deactivated. The MAC address is deleted from the display only after a Link-Up on the respective port or the Portsecurity Renew command. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SECURITY: The "PORT ERROR DISABLED" Security State was split up into "SECURITY DISABLED" and "LOOP DISABLED" depending on the indicated error status. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ERROR COUNTER: The function of the Error Counter was changed to suppress error packets which are mostly caused by the switching on/off of terminals. Additionally the Error Counter is incremented by 1 only if FCS Errors or Late Collisions have occurred within a 2-second-intervall. Previously the Error Counter was incremented by the absolute number of FCS or Late Collisions and thus could reach very high values, even if the error state was active for a short time only. With the new procedure it is now possible to exactly see in how many (2-second) time intervals errors have been counted. Thus it is easier to detect the duration of the error. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| DHCP/BOOTP: For the sake of conformity with RFC1034 the underline ("_") was replaced by a hyphen ("-") in the Factory Default name of the switch. Among others, this name is used in DHCP and BOOTP/TFTP requests. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SYSLOG: Now, for all event types 'Severity' can be individually configured (see Manager in the Device-Editor on the "Alarms -> Alarm Destinations" tab). | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CONSOLE: New command to refresh the DHCP IP parameter: "dh:cp ren:ew" | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| LLDP: LLDP-MIB according to IEEE802.1AB implemented. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: SNMP-FRAMWORK MIB implemented. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: Support implemented for reading the CLI configuration via Manager (see Manager in the Device-Editor under the "Configure" menu item). Note: This function is available only for switches with management hardware version 2 or higher and appropriate firmware. | | | ✓ **HW2,3** | ✓ **HW3** | | ✓ | ✓ |
| CONSOLE: New command to reload the switch configuration via DHCP/BOOTP: "dh:cp rel:oad-config". With this command no reboot will be executed and the new configuration will be activated On-the-fly. | | | ✓ **HW2,3** | ✓ **HW3** | | ✓ | - |
| SECURITY: New 'VLAN Authentication Mode' parameter implemented. This parameter is used to configure whether | | | ✓ | ✓ | | ✓ | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| authentication according to IEEE802.1X or MAC-based shall be deactivated (bypass function) for devices whose MAC addresses are detected in the Voice VLAN (IP-Phones). | | | | | | | |
| SECURITY: Two new parameters has been implemented:<br>- RADIUS Guest VLAN-ID (may be activated if the RADIUS server rejects the authentication)<br>- RADIUS Inaccessible VLAN-ID (may be activated if all RADIUS Server are down)<br>For a detailed explanation consult the new flowcharts within the corresponding chapters. | | | ✓ | ✓ | | ✓ | ✓ |
| SECURITY: The columns 'Active Default VLAN-ID' on WEB page 'Port State' and with TELNET/SSH/V.24 console command 'show interfaces' now shows the source of the Active Default VLAN-ID (Unsecure VLAN, Guest VLAN, Inaccessible VLAN, IEEE802.1X Authentication Failure VLAN, Port Default VLAN, RADIUS VLAN).<br>Note: This setting is relevant to ports with activated Portsecurity Mode with authentication via RADIUS server only (IEEE802.1X or MAC-based). | | | ✓ | ✓ | | ✓ | ✓- |
| RADIUS: New attribute 'NAS-PORT-ID' will be send to the RADIUS server on IEEE802.1X and MAC-Based Radius-Requests. | | | ✓ | ✓ | | ✓ | - |
| SECURITY: For Telnet and V.24 Console authentication via RADIUS server now the Timeout, Retries and the queried RADIUS server are indicated after entering name and password. | | | ✓ | ✓ | | ✓ | ✓ |
| SECURITY: SSHv2 implemented. This function requires management hardware version 3. | | | | ✓ | | ✓ | ✓ |
| RSTP: Enhancement of the compatibility with third-party manufactures e. g. Cisco PVST. Under certain circumstances the topology was periodically reconfigurated. | | | | ✓ | | ✓ | - |
| **Bugfixes Firmware:** | | | | | | | |
| - With activated Portsecurity and violation of the allowed number of MAC addresses the "More than three MAC's" state was wrongly sent to the Manager for all three MAC States.<br>- With switches of the GigaSwitch family under certain circumstances the MAC address list was not completely shown for the "sh:ow m:ac-address-table d:ynamic [a:ll]" Telnet command and the "Show MAC Table" Manager function. This problem was fixed. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| - With the automatic firmware check via BOOTP using the "tf:tp check-m:in-fw ..." or "tf:tp check-t:his-fw ..." command, when no update was necessary, an alarm with the error message "Error parsing loaded command line configuration - Line number = x" (x = line number of the CLI file) was wrongly sent. This problem only occurred if in the CLI file loaded via BOOTP an alarm IP address and the "TFTP Message" alarm were configured.<br>- With IEEE802.1X authentication the EAP-Success packet was send before the switch has moved the port to the VLAN-ID received by the RADIUS server. With very fast client PCs this may result in receiving the wrong IP address via DHCP. | | | ✓ | ✓ | | ✓ | - |

## 2.15. Release V3.59

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| DEVICE-EDITOR: New Function named "Ping from Device" on tab "MAC+Security State" implemented. | | | | | | | ✓ |
| DEVICE-EDITOR: The parameter "Portsecurity Failure Action" has been moved from the "Global" tab to the new tab "Security > Security Setup". | | | | | | | ✓ |
| DEVICE-EDITOR: New parameter named "Address Ageing for Portsecurity modes 'Disabled' and 'Auto allow...'" on tab "Security > Security Setup" implemented. For details refer to firmware manual. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| MASTER-EDITOR: Under rare circumstances after store and reload of a Master-Config it could occur that the checked parameters were lost. | | | | | | | ✓ |
| With some older Windows versions the Inventory function finishes with the error message "Could not find installable ISAM". This problem was fixed. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| LLDP/CDP: CDP/LLDP detail view per port. | ✓ HW2,3 | ✓ HW2,3 | ✓ HW2,3 | ✓ HW3 | ✓ | ✓ | ✓ |
| SWITCH: Cable diagnostic is now executable for GigaBit TP ports also. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| RSTP: Stability of Spanning Tree in combination with high broad/multicast traffic significantly increased. Additionally the Flow-Control function will be disabled if Spanning Tree is activated. This will garanty that the Spanning-Tree packets will be forwarded under all circumtances. All customers using Spanning-Tree should upgrade to this release. | | | | ✓ | | ✓ | - |

## 2.16. Release V3.58

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| DEVICE-LIST: New menu function for inventory. Here it is possible to export all information from the 'Agent' and 'Device Info' tabs to an Excel or XML file. | | | | | | | ✓ |
| DEVICE-LIST: New column under the title of "Spanning Tree" introduced. For devices with Spanning Tree support it is indicated whether all ports are set to Forwarding and how many ports are set to Discarding. Thus it is possible to easily see for ring configurations which device splits the ring in order to avoid a loop. | | | | | | | ✓ |
| DEVICE-LIST: The "Add Devices" menu item was renamed "Add/Remove" and extended by further commands for removing devices from the Device List. Previously these commands could only be executed via the right-click menu. | | | | | | | ✓ |
| DEVICE-LIST: New "Configure" menu item containing several commands for configuring the device. Previously these commands could only be executed via the right-click menu. | | | | | | | ✓ |
| DEVICE-LIST: Now you can jump to the beginning or the end of the list using the "Pos1" and "Ctrl-Pos1" or "End" and "Ctrl-End" buttons. As before you can use the "Up" and "Down" keys to scroll up and down page by page. | | | | | | | ✓ |
| DEVICE-LIST: In cells, which are displayed in yellow, because the contents has changed, when the mouse pointer comes near them now date and time of the change are indicated. | | | | | | | ✓ |
| DEVICE-LIST/EDITOR: Multi-user capability has been extended. This is particularly useful if the Manager is installed on different computers and these access the same server directories for database and device lists.<br>a) As son as a device is opened in a Device Editor for editing, the Manager now creates a Lock file for this device in the Database directory. If then a second Manager tries to edit the same device in parallel, an appropriate warning is issued indicating user name, PC name, date and time:<br>User [NDI\TheissenH]<br>on PC [WRH-PC0607]<br>is just editing this Device since [03.08.2008 09:06:34]<br>After leaving the Editor the Lock file is deleted again.<br>b) Under the "Extra > Preferences > Device-List" menu item a new "Autosave Device-List" configuration setting has been introduced. Here the interval for automatically saving the Device List can be configured. Only if changes are performed on the Device List, these will be saved in the defined interval. If a second Manager has opened the same Device List in parallel and wants to edit it, too, it will recognize the change performed by the first Manager and issue an appropriate warning: | | | | | | | ✓ |
| DEVICE-EDITOR: Improved clarity by changed representation from tabs to a tree menu with individual tabs. | | | | | | | ✓ |
| DEVICE-EDITOR: The temperature limits have been moved from the "Global" tab to "Alarms > Global Alarms". | | | | | | | ✓ |
| DEVICE-EDITOR: The "Industrial Alarm Setup" of the "Global" tab was moved to the new "Alarms > Industrial Alarms" tab and renamed "Industrial Alarm Output Setup". | | | | | | | ✓ |
| DEVICE-EDITOR: The parameters under "Industrial Alarm Outputs" on the individual port tabs have been moved to the new "Alarms > Industrial Alarms" tab and renamed "Link Down Alarms". | | | | | | | ✓ |
| DEVICE-EDITOR: The "Trap/Syslog Destination Table" was renamed "Alarm Destination Table" and now has its own tab called "Alarms > Alarm Destinations" so that all events can be displayed without scroll bar. | | | | | | | ✓ |
| DEVICE-EDITOR: The "Access" tab is now split into two separate tabs called "Management > Agent" and "Management Accounts". | | | | | | | ✓ |
| DEVICE-EDITOR: In all tables, where configuration settings can be made, the Read/Only cells have received a grey background. Cells, where settings can be made, have now uniformly a white background. Thus you can see at a glance for which cells of a table the configuration settings can be changed. | | | | | | | ✓ |
| DEVICE-EDITOR: A new "Password Encryption Mode" parameter is implemented on the "Accounts" tab. Here you can define whether the local passwords for the Admin and User account are saved in the device in their Standard format or as an MD5 hash. If the password is saved as an MD5 hash it is practically impossible to discover the actual password. Note: This function is only supported by firmware versions which also support Security features such as RADIUS and IEEE802.1X. | | | | | | | ✓ |
| DEVICE-EDITOR: Support of Cable Diagnostic implemented. For this purpose a new "Cable Diag. all TP Ports" button was | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| introduced on the "Global+Alarm State" tab and a new "Cable Diagnostic" button on the Port tabs. Using these buttons the diagnosis can be initiated optionally for all ports or for one single port only. Note: This feature is supported by selected switch types and firmware versions only. | | | | | | | |
| DEVICE-EDITOR: New buttons called "Select all Events" and "Clear all Events" have been implemented in the Trap/Syslog Destination Table. They allow you to select or delete all events of the respective destination with a single click. | | | | | | | ✓ |
| DEVICE-EDITOR: New "Alarms > SFP Alarms" tab. For SFPs alarm limits can now be defined for RX-Power, TX-Power and Laser-Bias-Current. If these limits are violated either SNMP traps or Syslogs messages are sent. Moreover the corresponding values are marked in red in the "Show SFP Info" function and the alarm is reported up to the "Alarms" column of Manager. | | | | | | | ✓ |
| DEVICE-EDITOR: New "SFP Event" event implemented. This event is transmitted, if an SFP was inserted or removed, or if one of the above "SFP Alarm Limits" was violated. | | | | | | | ✓ |
| DEVICE-EDITOR: - Support for industrial switches of the "E" series implemented. For these switches now the two input voltages and the status of the "Func." functional input are displayed on the "Global+Link State" tab. Moreover, for these inputs the corresponding alarms can be linked with the alarm outputs M1 and/or M2. This is done via the parameters in the "Industrial Alarm Output Setup" group on the "Alarms > Industrial Alarms" tab. | | | | | | | ✓ |
| DEVICE-EDITOR: Support for the "Enabled with LLDP forwarding to Uplink" mode is implemented on the "Discovery" tab for the "LLDP Mode" parameter. | | | | | | | ✓ |
| DEVICE-EDITOR: New "Clear Table" button implemented in the window for displaying the LLDP and CDP Neighbors using the "Show Neighbors" button. A click on this button will delete the Neighbor table. | | | | | | | ✓ |
| DEVICE-EDITOR: Now an automatic summer time correction can be enabled on the "Time Client" tab. | | | | | | | ✓ |
| LOGFILE: When updating the firmware after each 10 TFTP packets sent a dot is output as an activity indicator. | | | | | | | ✓ |
| GENERAL: The installation script for the Manager now aborts with an error message, if it was not possible to create one of the indicated sub-directories for firmware, master configs, etc. | | | | | | | ✓ |
| GENERAL: When launching the Manager the INI file is checked for integrity. In addition it is checked whether all subdirectories for firmware, master configs, etc. are available and can be written. In case of error, appropriate error messages are issued containing a hint on how to solve the problem. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| DEVICE-LIST: If the checkmark for "Uncheck successful Devices" was removed under "Update Firmware...", nevertheless all checkmarks were wrongly removed. | | | | | | | ✓ |
| DEVICE-LIST: For industrial switches with inserted MMC card with MAC address under certain conditions the "Active MAC Address" cell was displayed in yellow, although the MAC address was not changed. This problem was fixed. | | | | | | | ✓ |
| DEVICE-EDITOR: When a corrupt configuration was loaded into the Device Editor it could happen that the Manager crashed. In such cases the following error message is now issued:<br>Device Configuration corrupt!<br>Possible reasons are:<br>- Power disruption while Device stores Configuration to FLASH. Fix: Reset the Device to factory default.<br>- FLASH damaged. Fix: Replace management module or whole Device.<br>- If this error happens for all installed Devices the Manager version may be too old. Fix: Update Manager to current version. | | | | | | | ✓ |
| DEVICE-EDITOR: When a five-digit IP (e. g. "1.2.3.4.5") was entered into an entry field for an IP address and the "Database -> Save" command was executed, the Manager crashed. Now an appropriate error message is issued. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| SECURITY: For parameter 'Portsecurity Failure Action' it is now possible to select if the will be disabled after the first or second wrong MAC address. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LLDP: The Factory Default value for the LLDP Mode is now set to "disabled". | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| LLDP: New "Enabled with LLDP forwarding to Uplink" mode. With this setting LLDP packets, which have been received on a user port, are forwarded to all uplink ports. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LLDP: Support of LLDP-MED (ANSI/TIA-1057, LLDP for Media Endpoint Devices) implemented. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| LLDP: If an LLDP-MED terminal unit is connected, "LLDP-MED" is displayed under "Show Neighbors" as Discover type. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LLDP-MED: Transmission of the Voice LAN via LLDP-MED to an LLDP-MED-enabled terminal unit (e. g. IP phone) implemented. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TIME-CLIENT: Now an automatic summer time correction can be enabled for the SNTP client. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| CONSOLE: Without any exception, all parameters of the switch can now be configured via Telnet. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: New command for displaying the ARP table:<br>> sh:ow ar:p-table | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: New command for executing Cable Diagnostic:<br>> ca:ble-diagnostic {<if-no>\|a:ll} This command allows you to start the diagnosis optionally for all ports or for one single port. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: The 'poe-limit (1..100)' command was modified to 'config poe-limit (1..100)' for standardization purposes. Moreover the previous command for configuring the Spanning Tree port parameters:<br># rs:tp i:nterface <if-no> {mode} (prio) {cost-mode} (m-cost) {edge} {p-to-p}<br>was split up into individual commands for each parameter:<br># rs:tp i:nterface <if-no> ad:min-edge-port {n:o\|y:es-portfast}<br># rs:tp i:nterface <if-no> mo:de {e:nable\|d:isable}<br># rs:tp i:nterface <if-no> pa:th co:st-mode {r:stp-auto\|s:tp-auto\|m:anual}<br># rs:tp i:nterface <if-no> pa:th ma:nual-cost (1..200000000)<br># rs:tp i:nterface <if-no> po:int-to-point {y:es\|n:o\|a:uto}<br># rs:tp i:nterface <if-no> pr:iority (0..240)<br>IMPORTANT: The other commands for configuring the switch parameters were not changed in order to largely maintain compatibility with existing custom scripts. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: All previous 'show ...' commands for displaying the switch configuration have been converted to a uniform command syntax starting with 'show config ...'.<br>The following "show" commands have been newly introduced:<br># sh:ow con:figuration acce:ss [a:ll]<br># sh:ow con:figuration acco:unts [a:ll]<br># sh:ow con:figuration al:arm-destinations [a:ll]<br># sh:ow con:figuration ag:ent [a:ll]<br>> sh:ow con:figuration di:scovery [a:ll]<br># sh:ow con:figuration do:t1x [a:ll]<br>> sh:ow con:figuration g:lobal [a:ll]<br>> sh:ow con:figuration ig:mp [a:ll]<br>> sh:ow con:figuration in:terfaces [a:ll]<br>> sh:ow con:figuration p:riorisation [a:ll]<br># sh:ow con:figuration ra:dius [a:ll]<br>> sh:ow con:figuration rs:tp [a:ll]<br>> sh:ow con:figuration sf:p-limits [a:ll]<br>> sh:ow con:figuration sn:tp [a:ll]<br>> sh:ow con:figuration v:lan [a:ll]<br>Here, too, the function of the optional "all" parameter is identical with the above command:<br>'sh:ow ru:nning-config [a:ll]'<br>The following "show" commands are no longer available and have been replaced by the above commands:<br># sh:ow acce:sslist<br># sh:ow acco:unts<br>> sh:ow con:fig<br># sh:ow d:ot1x<br>> sh:ow ip<br>> sh:ow l:imiter<br>> sh:ow pr:iorisation<br>> sh:ow sn:tp<br>> sh:ow tr:ap-syslog | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| ACCOUNTS: The Admin and User passwords saved locally in the switch can now be saved alternatively as an MD5 hash. In order to activate this feature the new "Password Encryption Mode" parameter must be set from "Standard" to "MD5-Hash". | | | ✓ | ✓ | | ✓ | ✓ |
| CONSOLE: New command for displaying the running configuration:<br>sh:ow ru:nning-config [a:ll]<br>Without indication of the optional "all" parameter only settings deviating from factory default will be displayed. With indication of the "all" parameter additionally all configuration settings, also those set to factory default, are displayed. | | | ✓<br>**HW2,3** | ✓ | | ✓ | - |
| CONSOLE: New command for saving the running configuration to an external TFTP server:<br>> tf:tp <ip-address> p:ut <path> <filname.cfg> [a:ll]<br>The function of the optional "all" parameter is identical with the above command "sh:ow ru:nning-config [a:ll]". | | | ✓<br>**HW2,3** | ✓ | | ✓ | - |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| CONSOLE: The following "show" commands have been modified:<br>> sh:ow rs:tp {c:onfig\|s:tate}<br>This command was replaced by '> sh:ow rs:tp'. This command shows the current RSTP status. | | | | ✓ | | ✓ | - |
| Support for industrial switches of the "E" series. For these switches now the two input voltages and the status of the "Func." functional input are displayed in Telnet, WEB and NexManV3. Moreover, for these inputs the corresponding alarms can be linked with the alarm outputs M1 and/or M2. This is done e. g. in the Manager via the parameters in the "Industrial Alarm Output Setup" group on the "Alarms > Industrial Alarms" tab. | | | | | ✓ | ✓ | ✓ |
| SFP: For SFPs now alarm limits can be defined for RX-Power, TX-Power and Laser-Bias-Current. If these limits are violated, either SNMP traps or Syslogs messages are sent. Moreover the corresponding values are marked in red in the "Show SFP Info" function and the alarm is reported up to the "Alarms" column of the Manager. | | | | | ✓ | ✓ | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| SECURITY: - With firmware versions 3.55 and 3.56 the fixed MAC addresses of the "Learn and Fix one MAC Address" and "Learn and Fix two MAC Addresses" Portsecurity modes were deleted after a reboot. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Errors in connection with the "Show MAC Table" manager function removed. Under certain conditions the transmission of the MAC addresses from the switch to the manager was aborted early and the manager displayed a timeout. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |

## 2.17. Release V3.56

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Switch Firmware:** | | | | | | | |
| KONSOLE: Command to clear CDP/LLDP neighbor table implemented:<br>sh:ow n:eighbors-table [c:lear-table] | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| **Bugfixes Firmware:** | | | | | | | |
| CDP/LLDP: Under certain circumstances it could occur, that the switch reboots if he receives a CDP or LLDP packet with a long device name. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |

## 2.18. Release V3.55

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| Switch List renamed in Device List and Switch Editor in Device Editor, because NexManV3 will be able to manage fiber converters in future, too. | | | | | | | ✓ |
| The Preferences dialog box has been completely revised and structured. | | | | | | | ✓ |
| New 'Device' column in the device list, showing whether it is a switch or a fiber converter. | | | | | | | ✓ |
| New 'Alarms' column in the device list. This column shows how many of the following failure states are active:<br>- Temperature Failure<br>- Internal Voltage Failure<br>- PoE Input Voltage Failure<br>- Error Counter Failure<br>- Security Failure<br>- Loop Detection Failure<br>- Industrial Alarm | | | | | | | ✓ |
| New 'Location' column in the device list and at Layer-2 Autodiscover. Here the user-configured location is displayed. | | | | | | | ✓ |
| New 'Type column in the device list and at Layer-2 Autodiscover showing the type of device. | | | | | | | ✓ |
| New 'Mgmt Hardware Version' column in the device list and at Layer-2 Autodiscover. Here the hardware version of the management module is indicated. | | | | | | | ✓ |
| In the device list now a tool tip is shown for the 'Check' and 'Alarms' columns when the mouse is pointing onto the respective field. | | | | | | | ✓ |
| The device list is now permanently updated in the background by polling the devices. If a modification from the displayed list is detected, the corresponding value will be highlighted with a yellow background colour. If you then point the mouse onto yellow field, the old value will be shown. By closing and reopening the list or by right-clicking and choosing the 'Acknowledge changes of checked Devices' command, the values will again be highlighted with the default background colour. | | | | | | | ✓ |
| In the device list an arrow in the column header shows by which column the entries are sorted. The direction of the arrow indicates the ascending or descending order. Moreover you can define under Preferences by which column the sorting shall be performed when starting NexManV3. | | | | | | | ✓ |
| Now you can define under Preferences which columns shall appear in the device list. Additionally the order of the columns can be configured there. | | | | | | | ✓ |
| You can define under Preferences whether the column sizes of the device list shall automatically be adjusted to the contents of the fields. However, for the first polling run of the devices in the device list the sizes of the columns are principally determined automatically. If automatic adjustment is disabled, the width of the column can be changed by drawing the column header. Additionally the automatic adjustment can be disabled or enabled temporarily by the 'Adjust Column Size Automatically' check mark below the device list. | | | | | | | ✓ |
| New '[Check all parameters]' menu function implemented in the 'Master Editor'. When clicking on this function all parameters are selected for distribution. | | | | | | | ✓ |
| Now all parameters in the editor are displayed with pull-down settings and a corresponding arrow on the right margin: SNMP Trap . Before, it was not possible to recognize pull-down settings, in particular, within tables. | | | | | | | ✓ |
| New 'Discovery' tab in the Editor for configuring the Layer-2 discovery protocols CDP (Cisco Discovery Protocol) and the LLDP (Link Layer Discovery Protocol, IEEE802.1AB). | | | | | | | ✓ |
| New 'Show Neighbors' button on the 'Global+Link State' and 'Discovery' tabs in the Editor. When clicking on this button the detailed CDP and LLDP neighbour table will be shown. | | | | | | | ✓ |
| New 'DIP Switches Setup' parameters on the 'Access' tab in the Editor. Now the configuration switches of the management module can be disabled via a management function in order to prevent unauthorized manipulations by users. This only applies to cable duct and desk switches. | | | | | | | ✓ |
| Parameters for configuring the 'IGMP Querier' implemented on the 'IGMP' tab in the Editor. | | | | | | | ✓ |
| New 'Show RSTP State' button on the 'Global+Link State' tab in the Editor. When clicking on this button the detailed Spanning Tree Status will be shown. This button is also available on the 'RSTP' tab. | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| Extension of the parameter 'VLAN Attribute' by the 'IETF Tunnel-Private-Group-ID with VLAN-ID or VLAN-Name' on the 'Radius Auth.' tab in the Editor. With this setting the RADIUS server will accept both a VLAN ID and a VLAN Name. | | | | | | | ✓ |
| Extension of the 'Portsecurity Password' parameter by the tool tip 'leave empty to use MAC address' on the 'Radius Auth.' tab in the Editor. If this field is left empty, now the MAC address of the terminal unit to be authenticated will be used. | | | | | | | ✓ |
| The 'Description' column on the 'VLAN Table' tab in the Editor was renamed to 'VLAN-Name'. | | | | | | | |
| All parameters and tables in the Editor are combined by corresponding group frames in order to increase clarity. | | | | | | | ✓ |
| The automatic firmware update was extended so that the update will be repeated several times if failed due to a poor network connection. This prevents corrupt states of the switch firmware. | | | | | | | ✓ |
| All selection menus have been converted to WindowsXP styles. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| NexManV3 used to crash if you clicked in a 'Description' field of the 'VLAN Table' tab in the Editor (without entering text) and subsequently selected 'Database -> Save'. This problem was fixed. | | | | | | | ✓ |
| If the resolution of the screen display was set to 120dpi (instead of the default value of 96dpi) the input fields for the IP addresses were wrongly formatted. This problem was fixed. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| CDP: Support of the Cisco Discovery Protocol (CDP) implemented. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LLDP: Support of the Link Layer Discovery Protocol (LLDP) implemented. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The factory default switchname is now set to 'Aginode_xxxxxxxxxxx', whereas xxxxxxxxxxx will be replaced by the MAC address of the switch. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SWITCH: Now the configuration switches of the management module can be disabled via a management function in order to prevent unauthorized manipulations by users. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| DHCP: Now the name of the switch can be assigned via 'Host Name' DHCP option 12. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SECURITY: After changing the Portsecurity mode an automatic reset of all learned MAC addresses will be performed for the respective port. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SECURITY: If 'Portsecurity Failure Action' is set to 'Disable Port', now the first faulty MAC address will be blocked first. Only after the detection of a second faulty MAC address the port will be disabled. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SECURITY: For the Portsecurity function the status value 'Waiting for MAC Address' was added to the 'Security State'. This value shows that no MAC address has yet been detected for authentication. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| IGMP: Support of the IGMP querier function implemented. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| DHCP: Support of loading of configuration files via DHCP/BOOTP parameters implemented. Files containing console commands and binary files can be processed. | | ✓ **HW2,3** | ✓ **HW2,3** | ✓ | ✓ | ✓ | - |
| CONSOLE: Support of loading of configuration files via Telnet/V.24 console command implemented. Files containing console commands and binary files can be processed. | | ✓ **HW2,3** | ✓ **HW2,3** | ✓ | ✓ | ✓ | - |
| CONSOLE: Support of loading of a new firmware via Telnet/V.24 console command implemented. | | ✓ **HW2,3** | ✓ **HW2,3** | ✓ | ✓ | ✓ | ✓ |
| CONSOLE: Now a ping request can be performed from the Telnet/V.24 console to another device. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| CONSOLE: Commands for configuring Rapid Spanning Tree added. | | | | ✓ | | ✓ | - |
| SNMP/SYSLOG: New 'Internal Voltage Failure' event implemented. This event will be sent, if one of the two internal operating voltages is below or above the limit. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SNMP/SYSLOG: New 'TFTP Message' event implemented. This event will be sent in case of a successful or failed TFTP transfer of a configuration file. This does not apply to TFTP transfers which are directly performed by Aginode Switch Manager V3, since these will be documented in the Manager's log book. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SNMP: New version of Aginode MIB AGINODE.MIB (Version 3.6):<br>- bmSwitch: products {bmSwitch 35} added. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: New versions of the Aginode switch MIB NEX-BM.MIB (Version 3.7):<br>- bmSwitchPortTable:portSecurityForwardingState: enum (3) renamed from 'noLink' to 'waitingForLink'<br>- bmSwitchPortTable:portSecurityForwardingState: enum (5) | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| renamed from 'forwarding' to 'authenticated'<br>- bmSwitchPortTable:portSecurityForwardingState: enum (10)...(11) added<br>- Trap switchInternalVoltageFailure added.<br>- bmSwitchInfo: Object infoLastTftpMessage newly implemented.<br>- Trap tftpMessage newly implemented. | | | | | | | |
| Extension of the parameter 'VLAN Attribute' by the 'IETF Tunnel-Private-Group-ID with VLAN-ID or VLAN-Name' setting. With this setting the RADIUS server will accept both a VLAN ID and a VLAN Name. This is the new factory default of the device. | | | ✓ | ✓ | | ✓ | - |
| If no value is entered for the 'Radius Auth.' parameter of 'Portsecurity Password', now the MAC address of the terminal unit to be authenticated will be used. This is the factory default of the device. | | | ✓ | ✓ | | ✓ | - |
| Support of switch type 35 (iSwitch 742 SFP-I) implemented. | | | | | ✓ | ✓ | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| IGMP: Under certain conditions the conversion of a multicast MAC address to an IP address was not performed correctly with IGMP snooping. This problem was fixed. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: When retrieving the MAC address table via SNMP it might have happened in networks with many MAC addresses that the wrong port number was read for the MAC address. This problem was fixed. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SECURITY: Under certain conditions authentication was not triggered with IEEE802.X, in particular, if during authentication the TP cable was disconnected several times in a row. This problem was fixed. | | | ✓ | ✓ | | ✓ | - |

## 2.19. Release V3.52

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Bugfixes Firmware:** | | | | | | | |
| Under certain circumstances it could occur, that the switch doesn't accept the IP address received by DHCP. This problem has been fixed. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |

## 2.20. Release V3.51

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| The 'State' tab is now divided up into the three tabs 'Global+Link State', 'MAC+Security State' and 'PoE State'. Moreover, many status fields are presented in a colour representing their actual state. If the switch should go offline while the switch editor is open, the last received status values will continue to be indicated on the State tabs and a red message indicating the offline state will be shown. Previously the status values were deleted when offline. | | | | | | | ✓ |
| The previous 'Global' tab is divided into the two tabs 'Agent' and 'Global'. | | | | | | | ✓ |
| The individual parameters on the different tabs have been grouped in order to ease understanding. | | | | | | | ✓ |
| On the 'Global+Link State' tab the status display of the active voice VLAN is added. | | | | | | | ✓ |
| On the 'Global+Link State' tab the period of time elapsed since the last link change of the respective port is indicated for each port ('Time since last link change'). | | | | | | | ✓ |
| On the 'Global+Link State' tab the status display of the two operating voltages is added. | | | | | | | ✓ |
| On the 'Global+Link State' tab there is a new button 'Show SFP Info' for indicating the manufacturer and diagnostics information of all installed SFPs. This status information is supported e.g. by the new switch series 'GigaSwitch V2+' with SFP uplink and by iSwitch 1043. | | | | | | | ✓ |
| On the new 'MAC+Security State' tab now up to three MAC addresses per port are indicated (as already implemented in WEB and Telnet). Moreover, for each MAC address the 'MAC State' is shown informing on the current state of the authentication. This is especially relevant to the new Security modes with several IEEE802.1X instances per port. | | | | | | | ✓ |
| Furthermore the 'Show MAC Table' function is added to the 'MAC+Security State' tab. This function lists all dynamic and fixed MAC addresses including VLAN ID and port number. Subsequently the table shown can be sorted by MAC Address, VLAN-ID, Port No, Port Description or Port Name. Previously this function was available with Telnet only. | | | | | | | ✓ |
| On the 'MAC+Security State' tab the indication of the status of the Radius authentication and Radius accounting Servers is added. Previously this function was available with Telnet only. | | | | | | | ✓ |
| A new 'Radius Accounting' tab for configuring the Radius accounting parameters. These settings are relevant only from firmware versions V3.51 and with Radius support | | | | | | | ✓ |
| All VLAN settings previously arranged on different tabs have now been grouped on a new 'VLAN' tab. | | | | | | | ✓ |
| The new 'VLAN' tab can now be used to configure the voice VLAN per port which is supported from firmware version V3.40. Via this VLAN setting a single tagged VLAN, in particular for IP phones, can be configured for the respective port. In case of firmware versions with Radius support this VLAN can also be assigned via the Radius server. | | | | | | | ✓ |
| On the 'Global' tab now the temperature thresholds for generating a 'Temperature Event' (SNMP trap and/or SYSLOG message) can be configured. The previously fixed values of 0°C for 'Low Alarm Limit' and 70°C for 'High Alarm Limit' are now set as default values. | | | | | | | ✓ |
| On the 'SNMP+SYSLOG' tab there is a new 'Test Traps/Syslog' function for testing all SNMP traps and SYSLOG messages. Previously this function was available with Telnet only. | | | | | | | ✓ |
| On the 'SNMP+SYSLOG' tab the new 'SNMP MAC table mode' parameter is added. Here you can select whether the SNMP-retrievable MAC table shall list the addresses of all ports or only of the User ports. | | | | | | | ✓ |
| On the 'SNMP+SYSLOG' tab the two events 'RSTP New Root' and 'RSTP Topology Change' are added. These events are only relevant to switches with Rapid Spanning Tree support. | | | | | | | ✓ |
| On the '802.1X' tab parameters for configuring the new 'IEEE802.1X Client with MD5-Challenge' security mode are added. | | | | | | | ✓ |
| On the 'RSTP' tab there is a new button 'Show RSTP Info' for indicating the current Rapid Spanning Tree status. Previously this function was available with Telnet only. | | | | | | | ✓ |
| On the 'IGMP' tab there is a new button 'Show IGMP Info' for indicating the current IGMP port and router status. Previously this function was available with Telnet only. | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| On the 'PoE State' tab the 'Powerclass/max. Power (VA)' column was added in the 'Port PoE State' table. This status information is supported e.g. by the new switch series 'GigaSwitch V2+' and shows the power class according to IEEE802.3af as reported by the connected terminal. | | | | | | | ✓ |
| The switch-off period of the PoE voltage in case of a PoE reset was extended from two to six seconds. The switch-off time message on the port tabs was modified accordingly | | | | | | | ✓ |
| The new graphic styles for computers running the Windows XP or Vista operating systems were implemented. | | | | | | | ✓ |
| On the 'RSTP' tab the 'Name' column was added in the 'RSTP Port Setup' table. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| The temperature display in NexManV3 now also shows negative temperature values correctly. | | | | | | | ✓ |
| NexMan crashed when some numeric input fields were left empty and subsequently 'Save Config' was performed. This problem was fixed. | | | | | | | ✓ |
| Under certain circumstances NexMan crashed showing the error message 'Error during the creation of a windows handle'. This problem was fixed. | | | | | | | ✓ |
| If the switch editor was opened several times on the same PC, e. g. in order to configure different switches at the same time, after closing one editor it was not possible to write the configurations to the switches with the still open editors. An error message similar to 'Can't open file 'C:\Programme\Aginode\NexManV3\tmp\64_11_11_101-20070508214812.tmp'' was indicated. This problem was fixed. | | | | | | | ✓ |
| Under certain circumstances the switch editor was not re-opened after performing a [Write Config to Switch] operation. This problem was fixed in this release by using a workaround. In case of an error the switch editor is now opened and reset to its default size. A final bugfix will be implemented in the next release. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| Support of the following new status display functions of NexManV3.51 implemented:<br>- 'Voltage 1' and 'Voltage 2', internal operating voltages<br>- 'Time since last link change' per port<br>- 'Active Voice VLAN-ID' per port<br>- 'MAC Address 1'...'MAC Address 3', display of up to three Security MAC addresses per port<br>- 'MAC State 1'...'MAC State 3', for each MAC address the current authentication status is indicated<br>- 'Last Failure MAC Address', the last detected unacceptable MAC address per port<br>- 'Radius Server State', display of the status of the Radius authentication and Radius accounting server<br>- 'Show MAC Table', display of all dynamic and fixed MAC addresses, including VLAN-ID and port number<br>- 'Show SFP Info', display of the manufacturer and diagnostics information for all installed SFPs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The following statistics counters are set to 64 bit:<br>- Rx Unicast Pkts<br>- Tx Unicast Pkts<br>- Rx Broadcast Pkts<br>- Tx Broadcast Pkts<br>- Rx Multicast Pkts<br>- Tx Multicast Pkts<br>- Rx Octets<br>- Tx Octets<br>- Rx FCS Error Pkts<br>- Tx Late Collisions<br>An overflow of these 64-bit counters is virtually impossible. The 64-bit counter values are returned on all management interfaces, incl. the SNMP High-Capacity-Counter. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Implementation of a tagged voice VLAN. Via this VLAN setting a single tagged VLAN, in particular for IP phones, can be configured for each single port. In case of firmware versions with Radius support this VLAN can also be assigned via the Radius server. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The switch-off period of the PoE voltage in case of a PoE reset command was extended from two to six seconds. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| WEB: On all configuration pages writing the parameters via the 'Set' Button is acknowledged by a corresponding status message. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| The network driver was improved in such a way that the management processor reacts considerably more robust when a high number of broadcast or multicast packets is inserted. Previously too many broadcasts or multicasts could block access to management. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| Now the temperature thresholds for generating a 'Temperature Event' (SNMP trap and/or SYSLOG message) can be configured. The previous fixed values of 0°C for 'Low Alarm Limit' and 70°C for 'High Alarm Limit' are now set as default values. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Support of the status display functions 'Show IGMP State' of NexManV3 implemented. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The network driver was improved in such a way that the IGMP reacts considerably more robust when a high number of multicast packets is inserted. Previously too many broadcasts or multicasts could block processing of the IGMP protocol packets. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| New parameter 'SNMP MAC table mode' implemented. Here you can select whether the SNMP-retrievable MAC table shall list the addresses of all ports or only of the user ports. | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TELNET/V.24 Console:<br>- New command for display of the manufacturer and diagnostics information of all installed SFPs:<br>- sh:ow sf:p-info [<if-no>]<br>- New commands for configuration of the temperature alarm thresholds:<br>- c:onfig temp-l:ow-alarm (-20..20)<br>- c:onfig temp-h:igh-alarm (30..100)<br>- New command for configuration of the SNMP table mode:<br>- c:onfig snmp-m:ac-table-mode {a:ll-ports\|u:ser-ports-only} | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| New command for configuration of the voice VLAN-ID per port:<br>- in:terface <if-no> vo:ice-vlan-id (0\|1...4095) | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| New command for configuration of prioritisation:<br>- Global Priority Setup: 802.1p: c:onfig priority-d:ot1p (priority value=0..7) (queue=0..3)<br>- Global Priority Setup: IPv4/IPv6: c:onfig priority-i:p (priority value=0..63) (queue=0..3)<br>- Port Default 802.1p Priorityvalue: in:terface <if-no> priority-de:fault (priority value=0..7)<br>- Port IEEE802.1p Prioritisation: in:terface <if-no> priority-do:t1p {e:nable\|d:isable}<br>- Port IPv4/IPv6 Prioritisation: in:terface <if-no> priority-i:p {e:nable\|d:isable} | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: New version of Aginode MIB AGINODE.MIB (Version 3.5):<br>- bmSwitch: Switch types {bmSwitch 52...56} added. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: New versions of the Aginode switch MIB NEX-BM.MIB (Version 3.6):<br>- switchOverTemperature trap renamed in switchTemperatureFailure<br>- bmSwitchAdmin: adminSnmpMacTableMode object added.<br>- bmSwitchPortTable: portVoiceVlanId object added. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| Radius accounting implemented. In addition to Radius authentication, for Radius accounting there is a dedicated set of parameters available for configuring the Radius server. All counters are transmitted with 64 bits. Here the extended Radius attributes 'Acct-Input-Gigawords' and 'Acct-Output-Gigawords' are used. Thus an overflow of these counters can virtually be excluded. | | | ✓ | ✓ | | ✓ | ✓ |
| New 'IEEE802.1X PC+Voice allow two MAC Addresses' Security mode implemented. This mode enables the simultaneous authentication of a PC and an IP phone on the same port. The PC must be in the default VLAN and the IP phone in the voice VLAN of the respective port. | | | ✓ | ✓ | | ✓ | ✓ |
| New 'IEEE802.1X Multi-User allow three MAC Addresses' Security mode implemented. This mode enables the simultaneous authentication of up to three devices on the same port. All devices are assigned to the same default VLAN. | | | ✓ | ✓ | | ✓ | ✓ |
| New 'IEEE802.1X Supplicant with MD5-Challenge' Security mode implemented. This allows the switch to work as an 802.1X supplicant to the uplink and authenticate itself towards the core switch by EAP MD5-Challenge. | | | ✓ | ✓ | | ✓ | ✓ |
| New 'IEEE802.1X Radius MAC Bypass' Security mode. This enables the connection of either IEEE802.1X-ready clients OR 'dumb' terminals without having to change the port's Security mode. All switch ports can be operated in IEEE802.1X mode. | | | ✓ | ✓ | | ✓ | ✓ |
| TELNET/V.24 Console:<br>- New command for display of the Radius accounting configuration and the server status:<br>- sh:ow ra:dius ac:counting<br>- New commands for configuration of the IEEE802.1X and server status:<br>- sh:ow ra:dius ac:counting | | | ✓ | ✓ | | ✓ | - |
| Support of the status display functions 'Show RSTP State' of NexManV3 implemented. Display of the current Rapid Spanning Tree status. | | | | ✓ | | ✓ | ✓ |
| Display of the current Rapid Spanning Tree status via WEB interface implemented. | | | | ✓ | | ✓ | - |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| RSTP: 'RSTP New Root' and 'RSTP Topology Change' event types implemented (SNMP trap or SYSLOG message). | | | | ✓ | | ✓ | ✓ |
| The network driver was improved in such a way that the RSTP now is considerably more robust when a high network load of broadcast or multicast packets is present in the management VLAN. Previously too many broadcasts or multicasts could block the processor and delay the processing of the RSTP BDPUs. | | | | ✓ | | ✓ | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| When writing the switch configuration using NexManV3, ping requests to the switch could get lost during the activation of the new configuration. This problem was fixed. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| When logging in with the Read/Only Account on the WEB interface the per-port statistic counters could not be displayed. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| The temperature display in WEB, Telnet and SNMP now also shows negative temperature values correctly. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |

## 2.21. Release V3.30

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| New Autodiscovery feature "Autodiscover Switches on local segments". This function automatically detects all switches in the local segment, even if they do not have an IP address yet. Setting or modifying the IP address is possible directly from the Autodiscovery function. | | | | | | | ✓ |
| Display of statistics counters per port and for all ports added. When pressing the "Show statistic counter" button on a port tab, only the counters for this particular port are displayed. Moreover, this counter window is automatically updated every 5 seconds. When pressing the "Show statistic counter" button on the State tab, the counters for all ports are displayed. Pressing the "Refresh" button updates he counters. | | | | | | | ✓ |
| The switches are no longer polled via ICMP Echo (Ping), but exclusively via UDP port 50266. This avoids any problems with firewalls and ensures that it is a Aginode switch. | | | | | | | ✓ |
| NexConV3 is now installed together with NexManV3. A separate installation is only required, if only NexConV3 is needed on the respective PC (e.g. on the installer's notebook). | | | | | | | ✓ |
| New "WEB TCP Port" setting implemented on "Access" tab. The TCP port for WEB access can now be configured freely. | | | | | | | ✓ |
| The setting "Accesslist Mode" has been extended by the "Enable for SNMP access only" option on the "Access" tab. | | | | | | | ✓ |
| The new "TFTP authen. via SNMP" setting has been implemented on the "Access" tab. The download or upload of the configuration via TFTP and the update of the firmware via TFTP can now be authenticated alternatively via the new SNMP variable 'adminTftpAccess'. The corresponding mode for this authentication "TFTP access via SNMP" can be set to "Disabled", "Read/Only" or "Read/Write". | | | | | | | ✓ |
| The new "SNMP authentication mode" setting has been implemented on the "SNMP" tab. Here SNMP access can be set to "Disable", "Read/Only" or "Read/Write". | | | | | | | ✓ |
| The currently active MAC address is now shown under "Active MAC address" on the "State" tab. This is particularly relevant, if an MMC card with its own MAC address is used for the iSwitch. | | | | | | | ✓ |
| The "System up time" is now indicated on the "State" tab. | | | | | | | ✓ |
| The "Shared secret" is now indicated invisibly on the "Radius" tab. | | | | | | | ✓ |
| A new check box called "Renew" has been implemented on the Port tabs under "Port Security". By checking this box and subsequently executing the [Write Config to Switch] command a Renew of the respective port's Security function is executed. The check mark is automatically removed after execution of this function. | | | | | | | ✓ |
| A new check box called "Reset" has been implemented on the Port tabs under "Power over Ethernet". By checking this box and subsequently executing the [Write Config to Switch] command a Reset of the respective port's output voltage is executed. The check mark is automatically removed after execution of this function. | | | | | | | ✓ |
| The Telnet program to be executed after selection of the Switcheditor menu "Configure Switch > Open Telnet" can now be set under 'Extra > Preferences'. | | | | | | | |
| New IGMP tab for setting the IGMP Snooping Parameter for switches with IGMP support. | | | | | | | ✓ |
| New "Configure Switch > Write Config to Switch with fixed IP 172.23.44.111" feature has been implemented in the switch editor. This function allows you to transfer the configuration, which is currently loaded from the database, into a switch which was booted with the fixed IP address IP 172.23.44.111 using the configuration switch. When replacing a switch, this allows you to transfer the complete configuration of a switch to the replacement switch which does not need to have the old IP address before. | | | | | | | ✓ |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| The "Application data folder" defined during installation is now displayed under "Extra > Preferences". | | | | | | | ✓ |
| New menu entry in the "Add Switches" switch list. The functions indicated there can also be called by right-clicking. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| When saving the Master Config to the Mastereditor, NexManV3 might crash under certain circumstances and return the error message "The value for an unsigned byte was too big or too little". This problem was fixed. | | | | | | | ✓ |
| For the Swiss regional setting the PoE Power value was wrong on the "State" tab. This problem was fixed. | | | | | | | ✓ |
| Under certain conditions the IP address was deleted on the "SNMP/Syslog" tab. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| NexManV3: Support implemented for the new NexManV3.30 'Autodiscover Switches on local segment' function. This function automatically detects all switches in the local segment, even if they do not have an IP address yet. Setting or modifying the IP address is possible directly from the Autodiscovery function. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Access list: New 'Enable for SNMP only' setting option implemented for 'Accesslist mode'. Setting is possible via NexManV3 ('Access' tab) or Telnet: c:onfig ac:cesslist-mode {d:isable\|n:exman\|s:nmp\|a:ll} | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| WEB: Revision of the presentation and structure of the WEB pages. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: For iSwitch 1043: Info and diagnosis of the inserted SFPs can be displayed in WEB on the 'Port+Alarm State' page. To do so, click on the 'SFP Info' link in the 'Port Descr' column. | | | | | ✓ | ✓ | - |
| WEB: The TCP port for WEB access can now be configured freely. Setting is possible via NexManV3 or Telnet: c:onfig web-t:cp-port (1...65535) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| WEB: The 'Renew IP and VLAN parameter' command on the 'Switch Setup' WEB page is no longer executed via the 'Reset' command, but via a separate line by setting a check mark.. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: The 'Renew Security and enable Port' command on the 'Port state' WEB page is no longer executed via the 'Security' mode, but via a separate line by setting a check mark. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: The 'Reset Power' command can now be executed via WEB, too. To do so, just set the check mark for 'Reset Power' on the 'PoE State' page in the setup menu. After execution of the command the PoE output voltage is disabled for 2 seconds and afterwards automatically enabled again. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: Indication of the Flow Control implemented in WEB. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: After modifying the VLAN or IP parameters now a message is displayed on the 'Port State' WEB page informing that the 'Renew IP and VLAN parameter' command on the 'Switch Setup' page must be executed for activating the new settings. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: Indication of the Port Statistic counters in WEB. To do so, click on the 'All counters' link in the 'Error Counter' column. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: Indication of MAC addresses per port in WEB. Up to three MAC addresses per port are indicated in the 'Security Mode / [MAC Addresses]' column. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: The actually currently active VLAN-ID is now indicated on the 'Port State' WEB page in the 'Active VLAN-ID' column. After modifying the VLAN-ID in Port Setup the 'Active VLAN-ID' will temporarily be kept. Only after executing the 'Renew IP and VLAN parameter' command the configured VLAN-ID will be indicated as the active VLAN-ID. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| WEB: The actually currently active Trunking Mode is now indicated on the 'Port State' WEB page in the 'Active Trunking Mode' column. After modifying the Trunking Mode in Port Setup the 'Active Trunking Mode' will temporarily be kept. Only after executing the 'Renew IP and VLAN parameter' command the configured Trunking Mode will be indicated as the active Trunking Mode. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| NexMan: The 'Reset PoE' command can now be executed via NexManV3, too. To do so, set the check mark for 'Reset' on the corresponding port tab and execute [Write Config to Switch]. | | | | | | | ✓ |
| NexMan: The 'Renew Security' command can now be executed via NexManV3, too. To do so, set the check mark for 'Renew' on the corresponding port tab and execute [Write Config to Switch]. | | | | | | | ✓ |
| TELNET/V.24 Console: The Help function of the console was extended. Now it is possible to search for certain commands using the 'help [search-text]' commands. The '?' command now | | ✓ | ✓ | ✓ | ✓ | ✓ | - |

| Switch family ➔ | Office | | | | Industry | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | I-BASIC | I-PROFESSIONAL | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | - | PRO2 PRO3 | - |
| only lists a short version of the command. | | | | | | | |
| TELNET/V.24 Console: After modifying the VLAN or IP parameters a message appears at the Telnet prompt informing that the 'renew' command must be executed in order to activate the new settings. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| TELNET/V.24 Console: The time interval, after which an automatic logout is performed, is extended from 5 to 15 minutes. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: New configuration setting: 'SNMP access mode'. Here SNMP access can be set to 'Disable', 'Read/Only' or 'Read/Write'. Setting is possible via NexManV3 or Telnet: c:onfig sn:mp-access-mode {read-write\|read-only\|d:isable-snmp} | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: The private MIB 'AGINODE-MIB' was extended. Version 3.4 is now the current MIB version. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: The private MIB 'AGINODE-BM-MIB' was extended and modified. Version 3.4 is now the current MIB version. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: MIB variable for TFTP authentication has been added: adminTftpAccess | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| SNMP: MIB variable for displaying and configuring the 802.1X Authentication Fail VLANs has been added: adminDot1xAuthFailureVlanId | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| TFTP: The download or upload of the configuration via TFTP and the update of the firmware via TFTP can now be authenticated alternatively via the new SNMP variable 'adminTftpAccess'. The corresponding mode for this authentication 'TFTP access via SNMP' can be set to 'Disabled', 'Read/Only' or 'Read/Write' via Telnet or NexManV3. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| IGMP Snooping implemented. Configuration can be set via NexManV3 or Telnet:<br>ig:mp-snooping {e:nable\|d:isable}<br>ig:mp-snooping a:geing (10...65535)<br>ig:mp-snooping c:lear-tables<br>ig:mp-snooping v:ersion {1\|2\|3} {e:nable\|d:isable}<br>Currently the state can only be displayed via Telnet:<br>'sh:ow ig:mp-snooping {c:onfig\|s:tatus}' | | | | ✓ | | ✓ | ✓ |
| RSTP: Rapid Spanning Tree MIB implemented. | | | | ✓ | | ✓ | ✓ |
| SNTP: Simple Network Time Protocol implemented. Configuration can be set via NexManV3 or Telnet:<br>snt:p st:atus {e:nable\|d:isable}<br>snt:p se:rver-ip <ip-address><br>snt:p v:ersion (1..4)<br>snt:p i:nterval (0..65535)<br>snt:p b:rodcast {e:nable\|d:isable}<br>snt:p o:ffset (-720..720)<br>snt:p r:equest-now | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| The SNTP time is indicated in NexManV3 ('State' tab), in Telnet ('show info' command) and in WEB ('Info' page). Moreover the time is entered into all Syslog messages as a timestamp. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| When plugging certain terminal devices (mostly new PCs with Gigabit NICs) onto a cable-duct switch, sometimes no link was established. Only by rebooting the switch or the terminal device a renewed link was possible. This problem was fixed. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| The configured PoE power limit was not exactly complied with. Deviations of +/- 1VA were possible. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| The Syslog message 'Mgmt Auth. Failure' did not indicate the IP address of the PC which caused the failure. | | ✓ | ✓ | ✓ | ✓ | ✓ | - |
| If both Radius Sever IPs were not configured (IP address: 0.0.0.0) and the Telnet or NexManV3 authentication mode was set to 'Radius first, then local', no fallback to the local passwords was performed. This problem was fixed. | | | ✓ | ✓ | | ✓ | - |
| The Syslog message 'Radius Mgmt Auth. Reject' did not indicate the IP address of the PC which caused the failure. | | | ✓ | ✓ | | ✓ | - |

## 2.22. Release V3.21

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | | | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| Support for east European windows versions implemented | | | | | | | ✓ |
| Names, passwords and SNMP Communities are no checked for valid characters. In the case of entering wrong characters a error message is displayed showing the valid characters and special characters. | | | | | | | ✓ |
| The two tables „Port State“ and „Port PoE State“ on Tab „State“ have been extend by the user specified portname. | | | | | | | ✓ |
| The table „Port State“ on Tab „State“ has been extend by the current „Flow Control“ state. | | | | | | | ✓ |
| The current „Flow Control“ state is now displayed on the „State“ tab in the „Port State“ table. | | | | | | | |
| **Bugfixes Manager:** | | | | | | | |
| On operation systems, which only have DotNet 2.0 installed, the editor windows was not displayed correctly after [Read Switch] or [Write Switch]. | | | | | | | ✓ |

## 2.23. Release V3.20

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | | | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| The directory, where the NexManV3 stores his preferences file, is now selectable during setup. This directory is also used for storing log files and some temporary files. | | | | | | | ✓ |
| The IP address and switch name are now displayed in the headline of the switch editor. | | | | | | | ✓ |
| Support for "Flow Control Mode" setup implemented (see tab "Global") | | | | | | | ✓ |
| New tab "SNTP Client" for configuration settings of the "Simple Network Time Protocol". Furthermore the system time will be displayed at the "State" tab. These functions are only supported for special firmware versions. | | | | | | | ✓ |
| If the "NexMan authentication mode" is set to "Radius only" or "Radius first, then local", the NexManV3 displays now the new RADIUS state messages of firmware V3.20. These messages will be shown in the log window. | | | | | | | ✓ |
| Support for operation systems, which only have DotNet 2.0 installed, implemented | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| In some cases the switchlist was sorted wrongly | | | | | | | ✓ |
| The installation on a Win98SE PC has failed if the NexManV3 was installed with a valid license key | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| Support implemented for switch types<br>- 20 (FiberSwitch 1000 BM+)<br>- 21 (DualSwitch 1000 BM+ FO/FO)<br>- 23 (DualSwitch 1000 BM+)<br>- 24 (DualSwitch 1000 BM+ TP/TP) und<br>- 25 (CopperSwitch 1000 BM+). | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| If the NexMan Authentication Mode is set to Radius Only or Radius First, Then Local, now the appropriate RADIUS state messages are communicated to NexManV3. Thus NexManV3 shows, whether RADIUS authentication was rejected or timed out. | | | ✓ | ✓ | | | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| When the Trunking Mode of a port was set to Enabled Without Tagging, this mode was not correctly indicated in the WEB interface. | ✓ | ✓ | ✓ | ✓ | | | - |
| (Only for switches with Gigabit uplink and industrial switches): If an out-speed bandwidth limiter was enabled for one or more ports and if these ports were operated in half-duplex mode, the switch might have affected the data traffic on all ports under certain conditions. For these switch types, now the out-speed limiter is automatically disabled for the duration of a half-duplex connection. This is only relevant for twisted-pair ports, which are set to autonegotiation or fixed to 10HDX or 100HDX. | ✓ | ✓ | ✓ | ✓ | | | - |
| The RADIUS attribute Tunnel-Private-Group-ID, sent by a Cisco ACS server for setting the VLAN-ID, was not correctly analysed. | | | ✓ | ✓ | | | - |

## 2.24. Release V3.13

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | | | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| Support for Microsoft Windows Server 2003 OS implemented | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| The minimum PoE input voltage for PoE options A and C was reduced from 40V to 5V. Thus also PoE loads with a lower input voltage (e.g. 12V or 24V) can be operated. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| New console command for globally enabling/disabling flow control. This command is supported for all industrial switches (iSwitch) and switches with Gigabit uplink (FiberSwitch 1000, DualSwitch 1000 and GigaSwitch).<br>The corresponding command is: c:onfig f:low-control e:nable\|d:isable | | ✓ | ✓ | ✓ | | | - |
| New console command for indication of the current flow control state. This command is supported for all industrial switches (iSwitch) and switches with Gigabit uplink (FiberSwitch 1000, DualSwitch 1000 and GigaSwitch).<br>The corresponding command is: sh:ow f:low-control | | ✓ | ✓ | ✓ | | | - |
| A Reboot With Factory Defaults can now also be performed via Telnet and V.24 consoles.<br>The corresponding command is: rel:oad f:actory | | ✓ | ✓ | ✓ | | | - |
| **Bugfixes Firmware:** | | | | | | | |
| When updating firmware V1.xx/V2.xx to V3.11 the Trunking Mode was disabled for all ports. | ✓ | ✓ | ✓ | ✓ | | | - |
| The configuration of a VLAN description via WEB failed under certain conditions. | ✓ | ✓ | ✓ | ✓ | | | - |
| Under certain conditions the Telnet console was blocked and a reboot was needed to deblock it. | | ✓ | ✓ | ✓ | | | - |

## 2.25. Release V3.11

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | ENHANCED/ SECURITY | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | ES3 | | | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| German and English manuals are now implemented | | | | | | | ✓ |
| Tab "SNMP" renamed to "SNMP/Syslog" and support for Syslog server added | | | | | | | |
| New tab for configuration settings of "Rapid Spanning Tree" implemented (firmware ENHANCED/V3.xx needed) | | | | | | | ✓ |
| New function "Auto-Discover Switches by IP range" implemented | | | | | | | ✓ |
| Support for "Port Monitor" function for industrial switches implemented (see tab "Global") | | | | | | | ✓ |
| Support for Memory-Card function for industrial switches implemented (see tab "Info") | | | | | | | ✓ |
| Window size and window position are now preserved | | | | | | | ✓ |
| Sorting switch lists is now much faster | | | | | | | ✓ |
| New function "Remove unknown Switches from List" | | | | | | | ✓ |
| The IEEE802.1x Transparency function can now be enabled by user (see tab "802.1X") | | | | | | | ✓ |
| Configuration setting for "V.24 Authentication Mode" for industrial switches implemented (see tab "Access") | | | | | | | ✓ |
| Setting "Enabled without tagging" added for parameter "Trunking Mode" | | | | | | | ✓ |
| New function within master config editor: "Check all parameters of this page" and "Uncheck all parameters of this page") | | | | | | | ✓ |
| Support for firmware update of the ENHANCED firmware version implemented | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| Significant acceleration of access via WEB | ✓ | ✓ | ✓ | ✓ | | | - |
| Port Monitor function for FiberSwitch 1000 | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| Faster loop detection when using the Userport With Active Loop Protection setting under Link Type. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| Now IEEE802.1X transparency can be disabled/enabled via NexManV3 and Telnet/V.24 console. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| The Trunking Mode was extended by the optional setting Enable Without Tagging | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| The state indication for the Trunking Mode in NexManV3, WEB and Telnet was replaced by the Active Trunking Mode indication | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| Support of firmware versions with file extension '*.img'. This extension is used with firmware versions of the GigaSwitch and ENHANCED types. | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| Support of the Management Module Vers.02. | ✓ | ✓ | ✓ | ✓ | | | - |
| Significant acceleration of access via SNMP. | | ✓ | ✓ | ✓ | | | - |
| Each interface in the SNMP ifTable now has a unique separate MAC address. | | ✓ | ✓ | ✓ | | | - |
| Sending of events to a maximum of Syslog servers implemented | | ✓ | ✓ | ✓ | | | ✓ |
| The detection of link changes and the sending of the appropriate traps or Syslog messages is now performed within a few milliseconds (previously with a delay of up to 2 seconds) | | ✓ | ✓ | ✓ | | | - |
| New V.24 console authentication modes Radius Only and Radius First, Then Local implemented for industrial switches. | | | ✓ | ✓ | | | ✓ |
| Now each port uses a unique separate MAC source address when sending the EAP packets. | | | ✓ | ✓ | | | - |
| First released version with Rapid Spanning Tree support | | | | ✓ | | | ✓ |
| **Bugfixes Firmware:** | | | | | | | |
| The factory default DHCP hostname was wrongly communicated with two underscore characters after 'Aginode' ('Aginode__xxxxxxxxxxx'). This was corrected to one single underscore ('Aginode_xxxxxxxxxxx'). | ✓ | ✓ | ✓ | ✓ | | | - |
| Under certain conditions it was not possible to read the configuration of the switch via NexManV3. Only after a reboot the configuration could be read again. This problem was removed. | ✓ | ✓ | ✓ | ✓ | | | ✓ |

## 2.26. Release V3.03

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | | | | NexManV3 Switch Manager |

| **Bundle code ➔** | - | - | - | | | | - |
|---|---|---|---|---|---|---|---|
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| Optionally a new Admin name and Admin password can be entered for Write Switch and Copy Master. This makes sense when the current Admin account is changed by writing the switch or when the NexMan Authentication Mode is set from Local to Radius. | | | | | | | ✓ |
| The Aginode Local Configurator (NexConV3) can now be directly started from NexManV3 via the main menu option [NexConV3]. | | | | | | | ✓ |
| The Telnet settings are activated on the Access tab for switches containing firmware WEB/V3.xx. | | | | | | | ✓ |
| **Bugfixes Manager:** | | | | | | | |
| Writing the configuration using Write Switch failed, when the NexMan Authentication Mode was set to Radius. | | | | | | | |
| The software crashed when an empty IP address was entered. | | | | | | | ✓ |
| The software crashed when the Default VLAN-ID was changed for switches without VLAN Table. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| The syntax for the SNMP variables infoSecurityFailMacAddr and infoNewMacAddr have been changed to the DisplaySring type. This also applies to the portNewMacAddress, portSecurityFailure and radiusPortSecurityReject traps containing these variables. The private NEX-BM.MIB SNMP MIB has been modified accordingly and now has Version 3.1. | | ✓ | ✓ | | | | - |
| New Telnet command for setting the Link Down alarm feature for industrial switches:<br>'in:terface <if-no> [alarm1\|alarm2] [e:nable\|d:isable] | | ✓ | ✓ | | | | - |
| New Telnet command for displaying the alarm state for industrial switches:<br>'sh:ow al:arm' | | ✓ | ✓ | | | | - |
| Now the VLAN which was assigned via Radius is no longer taken over as the Default VLAN of the respective port, but assigned for the duration of the authenticated connection only. The Default VLAN configured in flash is retained and will always be assigned if no VLAN is specified via Radius-Accept. | | | ✓ | | | | - |
| **Bugfixes Firmware:** | | | | | | | |
| Under certain conditions a VLAN-ID appeared twice in the VLAN table. | ✓ | ✓ | ✓ | | | | - |
| Incorrect indication of the gigabit link state with the PortLinkState SNMP variable | | ✓ | ✓ | | | | - |
| The Telnet command '# p:oe-limit (1..100)' could not be executed. | | ✓ | ✓ | | | | - |

## 2.27. Release V3.01

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | | | | - |
| **Aginode Switch Manager V3 (NexManV3):** | | | | | | | |
| First formally released NexConV3 Release | | | | | | | ✓ |
| Completely revised user interface based on DotNet Framework. | | | | | | | ✓ |
| All switches in the currently loaded switch list are automatically pinged and displayed in green or red in the list. The polling interval can be adjusted. | | | | | | | ✓ |
| Unrestricted support of all switch types, in particular DualSwitches and switches with Gigabit ports (FiberSwitch 1000 und DualSwitch 1000). | | | | | | | ✓ |
| Variable number of ports due to dynamic creation of port tabs. | | | | | | | ✓ |
| Relevant parameters of the individual ports are dynamically shown/hidden. | | | | | | | ✓ |
| State tab with current indication of port and PoE state as well as of temperature. | | | | | | | ✓ |
| The current state is read via a Refresh button. | | | | | | | ✓ |
| Reset of Error and Statistics counters for one switch or a list of switches. | | | | | | | ✓ |
| Database with history function. After each change to the switch configuration the old configuration is stored in the History list and can be reloaded. The number of switch configurations, which can be archived for each switch in the History database, can be set via the Preferences menu. | | | | | | | ✓ |
| Simple management of master configurations. Any number of master configurations can be created, and with each master the selected switch parameters are stored for distribution. | | | | | | | ✓ |
| Different storage locations for switch lists, database, master configurations and firmware files can now be set via Preferences. | | | | | | | ✓ |
| Display of PoE Adapter Info on the Info tab. | | | | | | | ✓ |
| Support of all new configuration parameters of V3 firmware. | | | | | | | ✓ |
| Global: Portsecurity Failure Action<br>Global: Tagging Ethertype<br>Global: Life Packet Rate<br>Access: Telnet Authentication Mode → Telnet disabled<br>Access: Telnet Password Mode<br>Access: WEB Authentication Mode<br>Priorisation: Priority Scheme<br>SNMP: Eight trap destinations with 16 traps each, which can be individually enabled.<br>Radius: VLAN attribute<br>802.1x: Max. Authentication Retries<br>802.1x: Authentication Failure VLAN-ID<br>Port: Port Type<br>Port: Link Type<br>Port: Autocross/Autopolarity | | | | | | | ✓ |
| New tabs for better organisation of switch parameters.<br>Access<br>Priorisation<br>SNMP | | | | | | | ✓ |
| Log book now with coloured error descriptions. | | | | | | | ✓ |
| Log book closes automatically if no error has occurred (can be disabled). | | | | | | | ✓ |
| Warning in the log book, if the switch has disabled NexMan Authentication. | | | | | | | ✓ |
| **Switch Firmware:** | | | | | | | |
| Support of all switch types in WEB (in particular DualSwitches) | ✓ | ✓ | ✓ | | | | - |
| The WEB interface can now be disabled or set to Read/Only. | ✓ | ✓ | ✓ | | | | ✓ |
| Configuration and display of the Security parameters now also via WEB. | ✓ | ✓ | ✓ | | | | - |
| Periodic transmission of Life Packets. Important for core switches performing automatic VLAN assignment based on the received IP address.<br>The transmission interval can be specified:<br>1 min. (factory default), 10 min., 1 hr., 10 hrs. or Disabled | ✓ | ✓ | ✓ | | | | ✓ |
| -For each port a Link Type can be specified.<br>- User<br>- User with Active Loop Protection(active transmission of loop packets)<br>- Uplink/Downlink (the switch prevents port from being disabled) | ✓ | ✓ | ✓ | | | | ✓ |
| New Portsecurity features. | ✓ | ✓ | ✓ | | | | ✓ |

| Switch family ➔ | Office | | | | | | Manager |
|---|---|---|---|---|---|---|---|
| Firmware family ➔ | WEB | SNMP/ TELNET/ WEB | SECURITY | | | | NexManV3 Switch Manager |
| Bundle code ➔ | - | - | - | | | | - |
| - Manual setting three vendor MAC addresses<br>- Learn and fix one MAC address<br>- Learn and fix two MAC addresses | | | | | | | |
| The Default VLAN can be disabled for tagged ports. | ✓ | ✓ | ✓ | | | | ✓ |
| The factory default setting for Autocross/Autopolarity is now enabled for all TP ports. | ✓ | ✓ | ✓ | | | | - |
| The prioritization scheme can be specified:<br>- Strict Priority Queuing<br>- 8-4-2 Weighted Fair Queuing | ✓ | ✓ | ✓ | | | | ✓ |
| Now the Port Type is indicated:<br>- Internal Management Port<br>- 10/100 Mbps Twisted Pair<br>- 10/100/1000 Mbps Twisted Pair<br>- 100 Mbps Fiber Optic<br>- 1000 Mbps Fiber Optic | ✓ | ✓ | ✓ | | | | ✓ |
| Now Autocross/Autopolarity can be separately enabled/disabled. | ✓ | ✓ | ✓ | | | | ✓ |
| Gratuitous ARP function guarantees that the switch can be reached after change of IP address. | ✓ | ✓ | ✓ | | | | - |
| Support of NexConV3 (Aginode Local Configurator V3) implemented. | ✓ | ✓ | ✓ | | | | ✓ |
| Support of NexManV3 state display implemented. | ✓ | ✓ | ✓ | | | | ✓ |
| The WEB interface is now principally included in all firmware versions. | | ✓ | ✓ | | | | - |
| The Telnet interface can be disabled. | | ✓ | ✓ | | | | ✓ |
| The number of trap destinations has been increased from three to eight. | | ✓ | ✓ | | | | ✓ |
| All 16 trap types can be separately enabled/disabled. | | ✓ | ✓ | | | | ✓ |
| All port-related Telnet commands have been standardized. The standardized form now is as follows:<br>- interface <if-no> <parameter> <setting> | | ✓ | ✓ | | | | - |
| Several global Telnet commands have been renamed and standardized, e.g.:<br>- c:onfig m:irror {e:nable\|d:isable}<br>- c:onfig n:scm-auth-mode {n:one\|l:ocal\|r:adius\|b:oth-radius-local}<br>- c:onfig telnet-a:uth-mode {l:ocal\|r:adius\|b:oth-radius-local\|d:isable-telnet} | | ✓ | ✓ | | | | - |
| New Telnet Password Mode parameter with Visible setting. Allows support of one-time passwords, so that the entered password is displayed in plain text (only useful in connection with RADIUS). | | ✓ | ✓ | | | | ✓ |
| New Portsecurity features.<br>- IEEE802.1X allow multiple MAC addresses<br>- IEEE802.1X or RADIUS allow one MAC address | | | ✓ | | | | ✓ |
| IEEE802.1X has been extended by an Authentication Failure VLAN. A user who has entered a wrong password will be shifted into this VLAN. | | | ✓ | | | | ✓ |
| The Secure VLAN was renamed into Unsecure VLAN. The new name more adequately reflects the proper function of this VLAN. | | | ✓ | | | | ✓ |
| Via the VLAN Attribute setting it is possible to specify which RADIUS attribute shall be read for the configuration of the VLAN:<br>- Aginode Vendor Specific VLAN-ID<br>- IETF Tunnel-Private-Group-ID with VLAN-ID<br>- IETF Tunnel-Private-Group-ID with VLAN-Description<br>- Ignore VLAN attributes | | | ✓ | | | | ✓ |

Aginode networking solutions are employed all over the world and have demonstrated their reliability in a variety of applications. Our references include leading companies of the world, universities, industrial enterprises, hospitals, government authorities and banks. A LAN system which can grow with the requirements of its users must be designed from the very beginning in such away that it is flexible enough to support frequent moves, adds and changes, in particular.

**With more than 25 years of experience in the development and production of optical solutions, the systems from Aginode provide the reliability and the security you can expect from your network.**


**Aginode Germany GmbH**
Bonnenbroicher Str. 2-14 • 41238 Mönchengladbach
Tel +49(0)21662552010
Fax +49(0)21662552499
E-mail: sales.germany@aginode.net
https://www.aginode.net/en/Data/Products-Solutions/LANactive.html