# Aginode Switch Management
## with Firmware *V8.00L* and Manager *V8.00I* *or later*

Release Notes KD558E37

**CONTENTS**

# 1. Important Notice

- 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)

**HW5** = Function requires management hardware version HW5 or higher

## 2.1. Release V8.00

### 2.1.1. Release V8.00L

| **Switch family ➔** | **Office** | **Industry** | **Manager** |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager** |
| **Manager – Basic Features:** | | | |
| [from V8.00A]:<br>Support for multiple SQL database providers has been added. | | | ✓ |
| [from V8.00A]:<br>LANactive Manager is now completely platform independent and can run on Windows, MacOS, iOS, Android and Linux. | | | ✓ |
| [from V8.00A]:<br>Web-Interface now contains all possible functionalities and can be used instead of the Client application. | | | ✓ |
| [from V8.00A]:<br>A customizable Dashboard for showing all kinds of parameters in a graphical way, like Temperature, Alarms or any kind of event has been added to the manager. | | | ✓ |
| [from V8.00A]:<br>Positioning: Place devices on world map or building layouts. | | | ✓ |
| [from V8.00A]:<br>Added mew option to role templates, which allow users to modify categories inside their Device-Lists, even when they are not administrators | | | ✓ |
| [from V8.00A]:<br>From this version on, it is possible to modify single VLANs inside the VLAN table with master-configs. | | | ✓ |
| [from V8.00A]:<br>For Zero-Touch-Configuration, Default Configs can be assigned to IP Address Ranges, making it possible to provide different Default Configs for the same Switch family. | | | ✓ |
| [from V8.00B]:<br>'Reset All Filter' button has been added to Device-List. | | | ✓ |
| [from V8.00D]:<br>Google Maps has been added as map provider for Positining → Map. | | | ✓ |
| [from V8.00F]:<br>Added multiple configuration options to Active Directory settings to support different LDAP server providers. | | | ✓ |
| [from V8.00G]:<br>It is now possible to configure multiple switch default accounts for different IP Address ranges. | | | ✓ |
| [from V8.00I]:<br>Only selected and visible Device-Editor will poll device to increase performance and decrease traffic. | | | ✓ |
| [from V8.00I]:<br>Update performance of Device-List has been increased. | | | ✓ |
| [from V8.00I]:<br>Column for alarms located inside subcategories has been added to category tree. | | | ✓ |
| [from V8.00I]:<br>Settings → Controller → General: Setting for automatic logout of idle users has been added. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V8.00B]:<br>Syntax error in Linux Redhat Install Script has been fixed. | | | ✓ |
| [from V8.00B]:<br>Web Interface File Management now shows .xml files for Master-Configs. | | | ✓ |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager** |
| [from V8.00B]:<br>Active filter where not always marked in column header. | | | ✓ |
| [from V8.00B]:<br>When username contained '.', layouts where saved with firstname only. | | | ✓ |
| [from V8.00B]:<br>File names are now checked for invalid chars. | | | ✓ |
| [from V8.00B]:<br>Linux default log directory has been moved to $HOME/.local/share, similar to data directories. | | | ✓ |
| [from V8.00B]:<br>Passwords from unused connection strings stayed where not encrypted. This has been fixed. | | | ✓ |
| [from V8.00B]:<br>Linux: Changing the executing user during setup did not work properly. This has been fixed. | | | ✓ |
| [from V8.00C]:<br>Linux: Importing Device-Lists with long category names sometimes failed. | | | ✓ |
| [from V8.00C]:<br>Linux: LDAP authentication has been fixed. | | | ✓ |
| [from V8.00D]:<br>Client/Controller: Poll Engine did not poll new switches. | | | ✓ |
| [from V8.00E]:<br>Device-Editor → Security → Security Setup → Re-enable time for Security-Disabled ports could not be written. | | | ✓ |
| [from V8.00F]:<br>An error has been fixed which blocked opening the Device-Editor while multiple users are logged in. | | | ✓ |
| [from V8.00G]:<br>A problem has been fixed which caused automatic reset of Server Addresses in Device-Editor → Security → RADIUS Management Authentication. | | | ✓ |
| [from V8.00H]:<br>An error while saving session storage has been fixed. | | | ✓ |
| [from V8.00H]:<br>Dashboard: Combobox to select devices took long time to open, when database contains more than 1000 devices. | | | ✓ |
| [from V8.00H]:<br>Removed downloading of unnecessary googlemaps scripts. | | | ✓ |
| [from V8.00H]:<br>A problem leading to unencryptable database credentials on first service start has been fixed. | | | ✓ |
| [from V8.00H]:<br>A problem leading to unencryptable RADIUS Shared Secret has been fixed. | | | ✓ |
| [from V8.00I]:<br>When uploading multiple firmware files via Web-Interface during firmware update process, only the first file was selected for further process automatically. | | | ✓ |
| [from V8.00I]:<br>Estimated firmware update timespans have been corrected and thereby reduced. | | | ✓ |
| [from V8.00I]:<br>Manager was sometimes frozen when dialogs are closed with 'Esc'. | | | ✓ |
| [from V8.00I]:<br>New IP depend default accounts have been added to authentication window. | | | ✓ |
| [from V8.00I]:<br>Dashboard performance for lage number of switches has been increased. | | | ✓ |
| [from V8.00I]:<br>Upgrading old Master-Configs to V8 with encrypted passwords caused "invalid chars" error. | | | ✓ |
| **Firmware – Basic Features:** | | | |
| [from V8.00A]:<br>Only applies to V5 switches with management hardware version 5.4x or lower:<br>The Port Monitor has been extended so that more than one source port can be selected. I.e. packet traffic of one or more source ports can be mirrored to the selected destination port.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Global", the dropdown list "Portmonitor Source Ports" has been extended for selecting multiple source ports. | ✓ | ✓ | ✓ |
| [from V8.00A]<br>Only applies to 10/16-Port iSwitches with redundant input power S1/S2/S3:<br>New options to trigger a CLI script on power-up or power-down of the power sources S1, S2 or S3 have been added. For this purpose, the following CLI commands have been introduced:<br>- "cl:i-script p:ower {s1\|s2\|s3} {u:p\|d:own} a:ssign <CLI Script name>"<br>- "cl:i-script p:ower {s1\|s2\|s3} {u:p\|d:own} d:elete <CLI Script name>". | | ✓ | |
| [from V8.00A]<br>In the Alarm Destination Table alarm types and Syslog severities for Fabric Attach (FA) have been added:<br>- Fabric Attach VLAN Table Setup<br>- Fabric Attach VLAN Port Setup<br>Those alarms replace the corresponding Internal Mgmt Warnings 121 and 122.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "Alarms > Alarm Destination Tables in the Alarm Destination Table two rows for the alarm types "Fabric Attach VLAN Table Setup" and "Fabric Attach VLAN Port Setup" have been added. | ✓ | ✓ | ✓ |
| [from V8.00A]<br>Fabric Attach (FA) has been extended to forward the Management VLAN, if the switch has received the Management VLAN from an FA server or proxy. For this purpose, Fabric Attach (FA) Element TLVs are used to exchange Management VLAN between the switches via LLDP. To control, whether the Management VLAN shall be sent via LLDP, or be learnt via LLDP and set on the management port as Default VLAN, additional options Send Mgmt VLAN and Learn Mgmt VLAN have been introduced.<br>**Manager – Extensions:**<br>In the Device Editor, on tab "VLAN > VLAN Table", two checkboxes "Send Mgmt VLAN" and "Learn Mgmt VLAN" have been added. | ✓ | ✓ | ✓ |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager** |
| [from V8.00A]<br>Added parameters Syslog Port (1...65535, default 514) and Syslog Protocol (UDP, TCP, default UDP) to send Syslog messages to a Syslog Server. | ✓ | ✓ | ✓ |
| [from V8.00A]<br>Added Syslog according to RFC 5424 including new message format with extended timestamp and extra parameters (e.g. hostname, application name, PID). | ✓ | ✓ | |
| [from V8.00A]<br>DHCP relay feature has been added | ✓ | ✓ | ✓ |
| [from V8.00A]<br>The IEC61850 protocol stack has been enabled for V5 and V5.2 FTTO IND switches. | ✓<br>**FTTO IND** | | |
| [from V8.00A]<br>Only applies to FTTO GigaSwitches with V5 management hardware version 5.4 or lower:<br>Support for a new PoE++ head Rev.A has been implemented. | ✓ | | |
| [from V8.00C]<br>Support for the following industrial switch type with uplink MACsec encryption has been implemented:<br>88 iGigaSwitch 1002 E+ MACsec SFP-2VI | | ✓ | ✓ |
| **Firmware – Security:** | | | |
| [from V8.00A]<br>Fimware Downgrade Mode feature has been added to prevent downgrade of firmware<br>**Manager – Extensions:**<br>In the Device Editor, menu “Management->Agent”, a new feature “Firmware downgrade” to configure, firmware downgrade mode has been added. | ✓ | ✓ | ✓ |
| [from V8.00A]<br>Reduce access by read-only user to accounts and access configuration | ✓ | ✓ | ✓ |
| [from V8.00A]<br>MAC address has been added in the DHCP snooping log | ✓ | ✓ | ✓ |
| [from V8.00A]<br>Support for firmware updates with encrypted firmware images implemented. The firmware images [V8.00A to V8.00K] are not encrypted. Starting with firmware version V8.00L, all firmware images published on our support website are encrypted.<br>IMPORTANT:<br>To upgrade from a firmware version prior to V8.00A to an encrypted version, please upgrade to an 8.00 unencrypted version first. The unencrypted firmware version V8.00K is available on Aginode support portal. | ✓ | ✓ | |
| **Firmware – SNMP:** | | | |
| | | | |
| **Firmware – Redundancy:** | | | |
| | | | |
| **Firmware – Bug Fixes:** | | | |
| [from V8.00A]<br>If Zero Touch Configuration and DHCP was enabled. with DHCP options 6 (DNS Server Address) and 15 (Domain Name), the switch did not ask the DNS Server to resolve the "nexans-controller.[Domain Name]" to receive the LANactive Manager Controller IP Address. | ✓ | ✓ | |
| [from V8.00A]<br>If management access was authenticated via RADIUS or TACACS+ with a user name longer than 14 characters, the user name in the login message was truncated in the Local Log. The maximum length of a user name in the Local Log is now 64 characters for remote authentications. | ✓ | ✓ | |
| [from V8.00A]<br>Applies mainly to V5 GigaSwitches and XGigaSwitches with inserted memory card:<br>If the Memory Card Mode was set to "Enabled with AES-256-encryption and Firmware storage", on firmware upgrade the switch management access slowed down significantly and sometimes went offline for a while. | ✓ | | |
| [from V8.00A]<br>IEC61850 protocol didn’t work for V5 and V5.2 switches. | ✓ | ✓ | |
| [from V8.00A]<br>The PoE port LED changed to red if the PoE mode was set to "Disabled". Now the PoE port LED turns off. | ✓ | | |
| [from V8.00C]<br>TACACS+ Command Authorization was not working any more. CLI Command execution was rejected for all users independent from their permissions. | ✓ | ✓ | |
| [from V8.00D]<br>Only applies to 16-Port iGigaSwitches with management hardware HW5 and 10 or more copper ports:<br>When a PoE adapter iOption PoE+ 6/8P-30W with support of 8 PoE ports was installed, the PoE adapter was not found. | | ✓ | |
| [from V8.00D]<br>Only applies to 10-Port iGigaSwitches with management hardware HW5 and 6 or more copper ports:<br>When a PoE adapter iOption PoE+ 2/4P-30W with support of 4 PoE ports was installed, the PoE adapter was not found. | | ✓ | |
| [from V8.00E]<br>Aginode SFPs were not recognized as known SFPs. | ✓ | ✓ | |
| [from V8.00F]<br>Only applies to industrial switches with HSR ports and firmware version V7.07fk or higher:<br>It was not possible to establish a link on the HSR ports. | | ✓ | |
| [from V8.00K]<br>Broadcast DHCP packets were not redirected to the uplink when DHCP Snooping was activated | ✓ | ✓ | |

## 2.2. Release V7.06
## 2.2.1. 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 | | | ✓ |
| [from V7.06C]<br>The follwing values have been added to the SFP Inventory List:<br>Allowed Laser Bias Current Range (mA)<br>Measured Laser Bias Current (mA)<br>Allowed TX Output Power Range (dBm)<br>Measured TX Output Power (dBm)<br>Allowed RX Input Power Range (dBm)<br>Measured RX Input Power (dBm) | | | ✓ |
| [from V7.06C]<br>New setting “Poll Thread Pause Time” has been added. This settings forces every poll thread to wait for the given time before polling the next switch to reduce network traffic. | | | ✓ |
| **Manager – Bug Fixes:** | | | |
| [from V7.06A]:<br>Error with missing UserName in SwitchLock Table while opening the Device-Editor was fixed. | | | ✓ |
| [from V7.06C]:<br>Script files caused problem on switch when file did not end with linebreak. This has been fixed | | | ✓ |
| [from V7.06C]:<br>Device-Editor → Management → Banner: Banner text showed error message when text contains linebreak. This problem has been fixed. | | | ✓ |
| [from V7.06C]:<br>Device-Editor → Management → Agent: A problem has been fixed which caused an error after setting ‘Location’, ‘Contact’ or ‘Domain’. | | | ✓ |
| [from V7.06C]:<br>Device-Editor → Management → IP Setup: MAC Addresses could not be read from .csv file for setting IP when the MAC Address was not formatted with colons. This has been fixed. | | | ✓ |
| [from V7.06C]:<br>A bug has been fixed which caused the Web Interface to automatically logout the user. | | | ✓ |
| [from V7.06D]:<br>A bug has been fixed which prevented deleting of multiple log messages. | | | ✓ |
| [from V7.06E]:<br>Reading a Manager V8 config file caused the V7 Manager to delete this file, because it was recognized as corrupt. This has been fixed. | | | ✓ |
| [from V7.06E]:<br>Default Controller URL has been reset to http for better out-of-the-box performance. | | | ✓ |
| [from V7.06E]:<br>Cancelling speed of firmware update and configuration has been improved. | | | ✓ |
| [from V7.06F]:<br>Message-Authenticator Attribute was missing in RADIUS pakets. | | | ✓ |
| **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. | ✓ | ✓ | ✓ |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| [from V7.05re]<br>A Network Time Protocol (NTP) Client for protocol versions V1 to V4 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. | ✓ | ✓ | |
| [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 V7.06L]<br>Only applies 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. | ✓ | ✓ | |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| **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 the 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 GigaSwitche 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 GigaSwitche 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 GigaSwitche 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. 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. | | ✓ | |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| [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 V7.06L]<br>For the new delivered 100MBit Fiber SFPs (S/N 88646010-CE1) and 1GBit Fiber SFPs (S/N 88646015-CE1) wrong SFP info values were shown. | ✓ | ✓ | |
| [from V7.06O]<br>Only applies to V5 Office Switches with inserted memory card:<br>If the Config was written by LANactive Manager or CLI command, the switch management access slowed down and temporary went offline. | ✓ | | |

## 2.3. Release V7.04

### 2.3.1. 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”. | | | ✓ |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| [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:** | | | |
| | | | |
| **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. | ✓ | ✓ | |

| Switch family ➔ | Office | Industry | Manager |
|---|---|---|---|
| | | | |
| **Firmware family HW5➔** | **HW5-Fxx-Pxx-OFFICE** | **HW5-Fxx-Pxx-INDUSTRIAL** | **LANactive Manager V7** |
| [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. | ✓ | ✓ | |

## 2.4. Release V7.02

## 2.4.1. 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 | | | ✓ |

| 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** |
| [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. | | | ✓ |

| 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** |
| [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’. | ✓<br>**HW5** | ✓<br>**HW5** | ✓ |

| 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** |
| [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 | ✓ | ✓ | |

| 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** |
| [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** | |

| 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** |
| [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. | ✓ **HW5** | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | | ✓ **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. | ✓ **HW5** | ✓ **HW3** | |
| [from V7.02B]<br>Cisco phones did not accept the Voice VLAN that was assigned by Aginode switches via CDP. | ✓ | ✓ | |

## 2.5. Release V6.04

### 2.5.1. 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. | | | ✓ |

| 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** |
| [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. | | | ✓ |

| 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** |
| [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:** | | | |

| 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** |
| [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). | ✓ | ✓ | |

| 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** |
| [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** | |

| 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** |
| [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. | ✓ **HW5** | | |
| [from V6.03ez]<br>If the switch management received a ping request with routing parameters included, the management might hang up. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW3** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **HW5** | |
| [from V6.04Za]<br>Problems while applying customer pre-configuration in factory have been resolved. | ✓ | ✓ | |

| 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** |
| [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. | ✓ | ✓ | |

## 2.6. Release V6.02

## 2.6.1. 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'. | | | ✓ |

| 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 – 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** | ✓ |

| 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** |
| [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” | ✓ **HW5** | ✓ **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 | ✓ **HW5** | ✓ **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 | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | ✓ **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 $m \neq n$<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. | ✓ **HW5** | ✓ **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”. | ✓ **HW5** | ✓ **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. | ✓ **HW5** | | ✓ |

| 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** |
| [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** | ✓ |

| 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** |
| [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** | |

## 2.7. Release V5.04

### 2.7.1. 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. | | | ✓ |

| 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** |
| [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. | ✓ | ✓ | |

| 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** |
| [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 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. | ✓ | ✓ | |

| 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** |
| [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** | |

| 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** |
| [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** | |

## 2.8. Release V5.02

## 2.8.1. 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:** | | | |

| 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 | - |
| [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}` | ✓ | ✓ | ✓ |

| 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 | - |
| [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. | ✓ | ✓ | ✓ |

| 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** | **-** |
| [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. | ✓ | ✓ | |

| 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 | - |
| [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 | ✓ | ✓ | |

| 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 | - |
| [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. | ✓ | ✓ | |

| 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 | - |
| [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. | ✓ | ✓ | |

| 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** | **-** |
| [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. | ✓ | ✓ | |

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