MICROSENS

# Firmware Feature List

## Generation 6 Ethernet Switches

Firmware Version: V10.5.0

### General Architecture

| | | |
|---|---|---|
| Linux OS | The integrated Linux kernel provides state-of-the-art technology and support of relevant networking protocol standards. The Open Source architecture guarantees long-term support and availability. | Supported since: V10.1.0 |
| Advanced G6 Architecture | Code implementation is automatically derived from a central architecture definition. Design changes and updates are automatically propagated into all firmware modules and documentation leading to an inherently robust behaviour. All features are commonly shared among all user interfaces for seamless appearance. | Supported since: V10.1.0 |
| SD Memory Card | All firmware and configuration is stored on an accessible memory card with microSD form factor. By exchanging the memory card, the device configuration can be transferred in total from one device to another. Basic device data like MAC address and Article/Serial-No. are retained in an independent internal memory. Industry Switch uses a more robust standard SD card. | Supported since: V10.1.0 |
| Internal Memory Option | For devices with internal memory all firmware and configuration is stored internally. The SD card may be used for configuration and firmware backup. A boot option is provided to select Internal or SD preference. For highest security internal memory only can be chosen. | Supported since: V10.3.3 |

### Factory Information

| | | |
|---|---|---|
| Inventory and Factory information | Each device carries permanent information about its identity. This includes serial number, production codes, MAC address and a feature summary. These data are not located on the removable SD card. | Supported since: V10.1.6 |
| Custom Device Info | Permanent hardware coupled custom information string which may be used for inventory or location info. This information persists even when the SD card is exchanged. Custom data may be entered by the customer or devices can be ordered individually preset from factory according to customer request. | Supported since: V10.3.3 |

### System

| | | |
|---|---|---|
| Custom MAC address | While the MAC address is assigned at production time is possible to overwrite this MAC for special cases. | Supported since: V10.1.6 |
| Custom Inventory Data | The user can supply various private strings to customize the device. This includes port alias names (64 byte), system name, location and group strings (each 255 byte) plus a private inventory string of 512 byte length. | Supported since: V10.2.0 |
| Temperature Control | Temperature inside the device is monitored and actions are taken if required. There are warning events (Syslog, Trap) in several steps. Under severe condition the unit may reduce speed or power down some port to reduce heat dissipation. | Supported since: V10.1.6 |

## Hardware

| | | |
|---|---|---|
| Function | Fanless Layer 2+ Switch controlled by high speed 1Ghz ARM CPU. | Supported since: V10.1.0 |
| Green IT | State-of-the-Art chip technology supports Energy Efficient Ethernet (EEE) according to IEEE 802.3az.<br>Related norms: IEEE 802.3az | Supported since: V10.1.0 |
| Jumbo Frames | Supports Jumbo-Frames up to 10kBytes length. | Supported since: V10.1.0 |
| Modular Hardware Design<br>*Industrial Switch only.* | Modular in-field upgradable hardware design enclosed in sturdy stainless steel stackable unit. Especially compact device. | Supported since: V10.3.0 |
| RGB LED | Full color led indicators permit extensive yet easy to remember status decoding without any tools. Quiet mode turns of most led for unobstrusive operation. Lightshow mode helps to find a switch among others. | Supported since: V10.1.6 |
| Input / Output Pins<br>*Industrial Switch only.* | Two decoupled input pins and two relay outputs are available in the Industry Switch. All changes trigger events (Syslog, Traps). The input pins can also trigger user defined cli scripts file for flexible use. The relays may be triggered on power, redundancy or thermal problems. Relays and LEDs can be set to static or blink mode. Relays may also be controlled via scripts for full custom control. | Supported since: V10.3.0 |

## IP Stack

| | | |
|---|---|---|
| Dual Stack | Parallel handling of IPv4 and IPv6 protocol. | Supported since: V10.2.2 |
| IPv4 Stack | Internet Protocol v4 handling with support of IPv4, ARP, DHCP, ICMP.<br>Related norms: RFC 791 (IPv4), RFC 826 (ARP), RFC 792 (ICMP), RFC 793 (TCP), RFC 768 (UDP), RFC 2131 (DHCP) | Supported since: V10.1.0 |
| DHCP Options 66/67 | Unit configuration or software updates controlled via DHCP option 66/67 mechanism. A CLI script can be downloaded which in turn may request further download or configuration changes<br>Related norms: RFC 2131 (DHCP), RFC 2132 (DHCP Options), RFC 951 (BOOTP) | Supported since: V10.2.1 |
| IPv6 Management Access | Internet Protocol v6 handling with support of IPv6, DHCPv6, ICMPv6, NDP. IPv6 access to WEB, CLI, SNMP and NMP.<br>Related norms: RFC 2460/2464/3484/3513 (IPv6), RFC 2462 (Address Configuration), RFC 2463 (ICMPv6), RFC 2461 (Neighbor Discovery Protocol), RFC 3315 (DHCPv6) | Supported since: V10.2.2 |
| IPv6 Transport | IPv6 traffic can be transported via the switch. Filter options for enhanced security available. | Supported since: V10.2.0 |
| Dynamic ARP Inspection | Incoming ARPs are being verfied against IP/MAC relation database provided by DHCP snooping. In addition an access list (ACL) is used for verification. In addition too many ARPs can lead to the port being blocked to prevent ARP attacks. | Supported since: V10.5.0 |
| Secondary IPv4 Address | A secondary IP address may be assigned under which the management is alternatively available. | Supported since: V10.4.4 |

## Ethernet Port Features

| | | |
|---|---|---|
| Administration | Port control. For each port a 64 character long alias name can be assigned . | Supported since: V10.1.6 |
| Ethernet Twisted-Pair | Auto-Negotiation of speed 10/100/1000, duplex mode, flow-control, Auto MDI/MDI-X<br>Related norms: 802.3u, 802.3z | Supported since: V10.1.6 |
| Cable Tester | Integrated cable checker help discover broken cables. Technology is based on time domain reflection measurements of the cable. For each wire pair the termination status is determined. The cable length is calculated and cable shortcuts can be detected. | Supported since: V10.4.0 |
| Ethernet Fixed Fiber | 100/1000, duplex mode, flow-control | Supported since: V10.2.0 |
| Ethernet SFP | Support for pluggable optical port (SFP) permits use with various wave length, fiber types and link distances. Double SFP version MicroSwitch. Up to 8 SFP in Industry Switch. | Supported since: V10.2.0 |
| Dual Media Ports | Some ports can operate with copper or optical cable. Preferences and priorities can be selected. | Supported since: V10.2.1 |
| Loop Protection | Local loop protection detects parallel links to the same switch or loops between local ports to avoid endless packet storms. | Supported since: V10.3.2 |
| Egress Rate Shaping | Egress rate shaping may be use to limit the data traffic outgoing to an access port. | Supported since: V10.5.0 |

## SFP

| | | |
|---|---|---|
| SFP Management | SFP are automatically detected and their inventory data is displayed. Insertion and removal generates events that may be forwarded as Syslogs or Traps. | Supported since: V10.1.7 |
| Power Monitoring | The optical transmit and receive power is permanently monitored and events can be generated when the receive power level varies for more than a customer defined threshold. Automated delta detection eliminates the need to individually measure and configure each port during installation. | Supported since: V10.1.7 |
| CSFP Support | Some switch versions supports double port Compact-SFP optical interfaces. These SFP contain two independent single fiber channels and are displayed for two ports with independent optical data. | Supported since: V10.2.1 |

## Power-over-Ethernet (PoE)

| | | |
|---|---|---|
| PoE and Poe+ support | Up to 30W can be provided to the attached device. The total amount for power per unit depends on power supply and device type.<br>Related norms: 802.3af (PoE) 802.3at (PoE+) | Supported since: V10.1.6 |
| PoE Control | PoE / PoE+ voltage is turned on only after powered device (PD) is detected and classified on port. Output voltage and power is monitored. Port power is shut down if limits are exceeded. Events are generated to alert on PoE problems. | Supported since: V10.1.6 |
| PoE+ Enable | PoE+ should only be enabled through LLDP-MED protocol. The unit supports this but also permits PoE+ activation via configuration to support devices that do not support LLDP-MED. | Supported since: V10.2.1 |
| Emergency Port | Port can be assigned priority. Should PoE power limitation occur, the priority (emergency) port(s) are not shut down. | Supported since: V10.1.6 |
| PD Operation<br>*Industrial Switch only.* | The Industry Switch can be configured to operate on PoE. In this mode no other power supply is required. When one or two regular power supplies are connected, then the PoE input can act as secondary backup supply. | Supported since: V10.3.0 |

## Switch / MAC

| | | |
|---|---|---|
| MAC Table | The device supports up to 8192 MAC addresses. MAC addresses may be learned or manually configured. | Supported since: V10.1.0 |
| MAC Filter | Various display filter permit access to table of MAC addresses known to the switch. Predefined plus custom filter to search mac table are provided. | Supported since: V10.2.0 |
| SNMP Access | D-BRIDGE and Q-BRIDGE MIBs are supported.<br>Related norms: RFC1493 (obsoltes RFC1286) | Supported since: V10.2.2 |
| MAC Limit | Limit number of allowed MAC addresses per port. Independent of other port access control functions. | Supported since: V10.5.10 |
| Configurable MAC Aging Time | MAC aging time can be configured between 15s and 1 hour. Defaults to 5 minutes. | Supported since: V10.4.0 |

## RMON Statistics

| | | |
|---|---|---|
| RMON counters | 35 integrated counters per port for detailed traffic analysis and network trouble shooting.<br>Related norms: RMON: RFC 2819 (obsoletes RFC 1757, RFC 1271), Etherlike: RFC 2665 (obsoletes RFC 1643, RFC 1623, RFC 1398), RFC 2233 (obsoletes RFC 1573, RFC 1213) | Supported since: V10.1.7 |
| Port Utilization | For each port the utilization in % is shown independantly for each direction. A current utilization is shown as well as averaged values over 30s and 5 minutes. | Supported since: V10.2.3 |

## Virtual LANs (VLANs)

| | | |
|---|---|---|
| VLAN Filter | Up to 256 VLAN's may be configured.<br>Related norms: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p | Supported since: V10.2.0 |
| Access Mode | For the connection of non-VLAN capable end devices (e.g. PCs). Outgoing packets are sent untagged. Incoming packets are tagged with the port default VLAN ID (PVID). | Supported since: V10.2.0 |
| Trunk Mode | For the interconnection of VLAN capable switches. Outgoing packets are always sent tagged. Incoming packets are received tagged. Incoming packets without VLAN tag are tagged with the port default VLAN ID (PVID). | Supported since: V10.2.0 |
| Hybrid Mode | For the connection of VLAN capable and non-VLAN capable devices on the same port (e.g. VoIP-phone (tagged) and PC (untagged)). Outgoing packets are sent tagged, except packets for the port default VLAN ID (PVID), which are untagged. Incoming packets are received untagged for the port default VLAN (PVID), all other packets are tagged. | Supported since: V10.2.0 |
| Multiple VLAN Reservation Protocol (MVRP) | Multiple VLAN Reservation Protocol. This protocol automates and centralizes VLAN assignment in large networks.<br>Related norms: IEEE 802.1ak | Supported since: V10.5.0 |
| Priority Override | VLAN priority code point of incoming packets can be overwritten with the VLAN specific priority defined in the VLAN filter. | Supported since: V10.1.7 |
| Voice VLAN | VLAN ID used by LLDP/CDP to assign VLAN to connected VoIP-phone. | Supported since: V10.1.7 |
| RSTP VLAN | VLAN ID used by Spanning Tree instance for BPDU tagging. | Supported since: V10.1.7 |
| Unauthorized VLAN | VLAN ID assigned by Port Based Access Control to unauthorized ports (guest VLAN). | Supported since: V10.1.7 |
| Management VLAN | VLAN ID used by the management agent (device internal port). | Supported since: V10.1.7 |

## Quality of Service (QoS)

| | | |
|---|---|---|
| Priority Queues | 4 priority queues per port. | Supported since: V10.1.6 |
| Prioritization Scheme | Strict priority (higher priority always first) or weighted fair queuing (8:4:2:1 highest to lowest). | Supported since: V10.1.6 |
| Layer1 Priority | Static priority queue can be assigned for each port. | Supported since: V10.1.6 |
| Layer2 Priority (802.1p) | Incoming packets are forwarded according to the priority code point in their VLAN tag. The 8 VLAN priority code points can be individually mapped on the 4 priority queues.<br>Related norms: IEEE 802.1p (VLAN priority code point) | Supported since: V10.1.6 |
| Layer3 Priority (IPv4 / IPv6) | Incoming packets are forwarded according to the value of the DiffServ Codepoint (IPv4) / TrafficClass (IPv6) in their IP header. Maximum 64 codepoints are supported. For each code point the corresponding priority queue can be mapped.<br>Related norms: RFC 2474/3260 (IPv4 DiffServ/IPv6 Traffic Class) | Supported since: V10.1.6 |

## Spanning Tree Protocols

| | | |
|---|---|---|
| Spanning Tree (STP) | Automatic detection of loops and redundant network paths. Single STP instance running in configurable VLAN. | Supported since: V10.2.0 |
| Rapid Spanning Tree (RSTP) | Automatic detection of loops and redundant network paths. Rapid Spanning Tree Protocol (RSTP) is backwards compatible to Spanning Tree standard (STP) but uses a faster algorithm.<br>Related norms: IEEE 802.1D-1998 IEEE 802.1D-2004 | Supported since: V10.2.0 |
| Multiple Spanning Tree (MSTP) | Up to 64 STP instances running in configurable VLAN groups.<br>Related norms: IEEE 802.1Q | Supported since: V10.3.2 |
| BPDU Guard | BPDU guard monitors if STP protocol is running on a local access port and removes such packets. Option to shut down the port for security or to just send an event. | Supported since: V10.3.0 |
| Bridge Assurance | Detects unidirectional link failures that may occur with fiber optic links whereby one fiber direction breaks. | Supported since: V10.3.2 |

## Port Access Control

| | | |
|---|---|---|
| IEEE 802.1X Authentication | Multiple users can be authenticated using central RADIUS server based on username/password or certificate.<br>Related norms: EAP-PEAP/MSCHAPv2, EAP-PEAP/TLS, EAP-PEAP/MD5, EAP-TTLS/EAP-MD5, EAP-TTLS/EAP-MSCHAPv2, EAP-TTLS/MSCHAPv2, EAP-TTLS/EAP-TLS, EAP-TTLS/PAP | Supported since: V10.2.1 |
| RADIUS MAC Authentication | Multiple users can be authenticated using central RADIUS server based on their MAC addresses.<br>Related norms: EAPOL, RADIUS | Supported since: V10.2.1 |
| MAC locking | Multiple users can be authenticated based on their MAC addresses. Unlimited MAC addresses can be configured manually or automatically. Possibility to mix and match vendor MACs and specific MACs | Supported since: V10.2.1 |
| MAC learning | Up to 9 MAC addresses may be learned per port. Learned addresses are stored in the configuration. MAC learning can be preset prior to roll out. Simply the first n devices connected are automatically learned. | Supported since: V10.2.1 |
| Learned MAC time out | Time out of learned MACs to allow another computer to connect in MAC locking environment. | Supported since: V10.4.0 |
| Dynamic VLAN | RADIUS server can provide user specific VLAN ID using tunnel-attribute in accept message. Port VLAN is dynamically set accordingly. Unauthorized users may be placed in an unauthorized VLAN ('guest VLAN') or blocked completely. VLAN 4096 can be specified to indicate port default VLAN. | Supported since: V10.2.1 |

## IGMP

| | | |
|---|---|---|
| IGMP Snooping | Snooping of Internet Group Management Protocol (IGMPv1/ v2/v3) for IPv4. Automatic detection and forwarding of IPv4 multicast-streams. Unregistered packets can be flooded or blocked. Multicast routers can be detected by discovery or by query message.<br>Related norms: RFC 4541 (IGMP) | Supported since: V10.2.0 |
| IGMP Snooping per VLAN | Automatic detection and forwarding of IPv4 multicast-streams independent for each configured VLAN. | Supported since: V10.3.0 |
| MLD Snooping | Snooping of Multicast Listener Discovery (MLDv1/v2) for IPv6. Automatic detection and forwarding of IPv6 multicast-streams. Multicast routers can be detected by discovery or by query message.<br>Related norms: RFC 3810/4604 (MLD), RFC4541 | Supported since: V10.3.2 |

## DHCP

| | | |
|---|---|---|
| DHCP Snooping | DHCP snooping records IP addresses, VLAN information, etc. to record trusted interfaces. DHCP snooping supresses DHCP traffic from untrusted interfaces. | Supported since: V10.5.0 |
| DHCP Filtering | DHCP Filtering prevents DHCP being injected from a user port. This feature acts on IPv4 and IPv6 alike. | Supported since: V10.5.0 |
| DHCP Flooding Detection | Attempts to detect a DHCP attack and shuts down the access port when too many DHCP messages ingress on the port. | Supported since: V10.5.0 |
| DHCP Options 66/67 | Unit configuration or software updates controlled via DHCP option 66/67 mechanism. A CLI script can be downloaded which in turn may request further download or configuration changes<br>Related norms: RFC 2131 (DHCP) | Supported since: V10.2.1 |
| Dynamic ARP Inspection | Incoming ARPs are being verfied against IP/MAC relation database provided by DHCP snooping. In addition an access list (ACL) is used for verification. In addition too many ARPs can lead to the port being blocked to prevent ARP attacks. | Supported since: V10.5.0 |

## Network Time Protocol (NTP)

| | | |
|---|---|---|
| NTP Client | Network time is automatically retrieved from NTP server. Two NTP server may be specified. The clock mal also manually be set if NTP access is not desired.<br>Related norms: RFC 4330 (SNTP) | Supported since: V10.1.7 |

## Redundant Ring Protocol

| | | |
|---|---|---|
| MICROSENS Ring Protocol<br>*Industrial Switch only.* | MICROSENS ring redundancy protocol. Up to 2 independent rings can be handled by a single device simultaneously. Typical 50ms ring recovery upon break of a ring is provided. | Supported since: V10.4.1 |

## Link Layer Discovery Protocols (LLDP, CDP)

| | | |
|---|---|---|
| LLDP reception | Receive LLDP information from neighboring devices per port. Display retrieved information via all NMS interfaces. This includes geographical coordinates and civic location information.<br>Related norms: IEEE 802.1AB (LLDP) | Supported since: V10.2.1 |
| LLDP transmission | Geographical coordinates and civic location information can be specified for transmission to neighboring devices. | Supported since: V10.2.1 |
| LLDP-MED | Media Endpoint Discovery for the auto-discovery of LAN policies. Support of VLAN advertising and PoE+ control.<br>Related norms: ANSI/TIA-1057 (LLDP-MED) | Supported since: V10.2.2 |
| LLDP/CDP preference | Device will prefer standards based LLDP but will automatically accept CDP if present. | Supported since: V10.2.0 |
| CDP operation | Support for Cisco Discovery Protocol CDP v1, v2 for automatic detection of capabilities of neighbor CDP enabled devices. | Supported since: V10.2.0 |
| CDP Voice VLAN | Support of Voice VLAN for configuration of connected Cisco VoIP-phone. | Supported since: V10.2.0 |

## Link Aggregation Control Protocol (LACP)

| | | |
|---|---|---|
| Static Link Aggregation | Multiplies available bandwidth between two end points. The setup is manually.<br>Related norms: IEEE 802.1ax, IEEE 802.3ad | Supported since: V10.3.2 |
| Dynamic Link Aggregation | Multiplies available bandwidth between two end points. The setup is dynamic within a predefined group of ports.<br>Related norms: IEEE 802.1ax, IEEE 802.3ad | Supported since: V10.3.2 |
| Load Balancing and Trunking | Load balancing between ports that have the same path increases throughput and provides a backup link upon failure. Also known as EtherChannel (in LACP mode). | Supported since: V10.3.2 |

## Command Line Interface (CLI)

| | | |
|---|---|---|
| Base Features | Intuitive command line interface to manage every aspect of the device. Supports wildcards and named ports as variables. Quick command entry due to auto-completion and command recall buffer. Individual console prompt string, Console inactivity timeout automatically logs out unattended terminal. Supports color displays. Online help for each parameter by typing a ?. | Supported since: V10.1.5 |
| Context Sensitive Help | Type ? anywhere while editing and context sensitive help regarding the current parameter is provided. | Supported since: V10.1.5 |
| Offline Configuration | Offline configuration permits editing of an unlimited number of user configuration sets. These configurations may be copied, viewed, up and downloaded by file transfer protocols. Offline configurations can be made online at any time. | Supported since: V10.1.6 |
| Comprehensive Editing | All parameter are shown and edited with the same syntax. No handbook needed for operation. Command options can be scrolled. For numbers values ranges are shown. Parameter can be written for ranges or wildcards. | Supported since: V10.1.5 |
| Scripting | Supports full scripting and editing of script files. A script may execute any CLI command provided the access rights are valid. Scripts may locally be edited or downloaded. A script may also be downloaded by DHCP/BOOTP function when a unit is newly connected to the network. Such script may reconfigure the device, load other scripts or even download and install a software update. | Supported since: V10.1.7 |
| microScript Language | Powerful and comprehensive script language permits customized active functions which greatly increase flexibility of the product. | Supported since: V10.3.1 |
| Show All Config | With the ShowAllConfig command the entire configuration can be displayed to console and simultaneously to a script file. The script can be used as backup or to configure other units. The command may also be used to display only the differences to any stored or default configuration. | Supported since: V10.2.1 |
| Show All Status | With the ShowAllStatus command the entire status of any parameter is displayed to console and simultaneously to a script file. | Supported since: V10.4.1 |
| Create Snapshot | Creates a snapshot of all relevant system information inluding all config, status, internal process details. | Supported since: V10.4.1 |
| Live Syslog | Syslog events can be forwarded to the active console the moment they occur. Filtering according to logging setup applies.<br>Related norms: RFC3164 | Supported since: V10.2.0 |
| Telnet | A telnet session automatically invokes the cli. Telnet may be disabled in total or per user to enforce use of the more secure SSH method.<br>Related norms: RFC 854 (Telnet) via TCP/IP port 23. | Supported since: V10.1.7 |
| Secure Shell (SSH) | An SSH session automatically invokes the cli. SSH may be disabled by configuration.<br>Related norms: SSH via TCP/IP port 22. Authentication methods: RSA, Diffie-Hellman Key Exchange. Encryption protocols: 3DES-CBC, HMAC-SHA1. | Supported since: V10.1.6 |
| Welcome Message | A customer programmable welcome message can be defined. This is shown prior to login prompt. May also be used to indicate warning to deter malicious user. Multiline output supported. | Supported since: V10.3.2 |
| Umlaut Support | Support for German Umlaute, French Accents, etc. in all user interfaces for selected parameters. Supports ISO 8859-1 coding. | Supported since: V10.4.1 |

## Login Access Protection

| | | |
|---|---|---|
| Unlimited number of Users | Three default users are created and any number of additional users may be created. | Supported since: V10.1.6 |
| View Based Access Model | Access right can be precisely tailored for each user. Similar to SNMP V3 view model but applied to all user interfaces including CLI. | Supported since: V10.1.6 |
| General access rights | For quick and effective rights management the general read/ write privileges of a user can be selected. | Supported since: V10.1.6 |
| Disable Insecure Interfaces | It is possible to restrict management access to secure interfaces such as HTTPS, SSH, SNMP V3 | Supported since: V10.1.6 |
| Interface Restrictions | For each user the permitted user interfaces can be selected. | Supported since: V10.1.6 |
| Public key encrypted passwords | For each user an access password plus an SNMP V3 password is assigned. Proper AES256 public key encrpyted passwords are stored. | Supported since: V10.1.6 |
| View Model for SNMP V1,V2c | The access view model may be applied to SNMP V1 or V2c access, practically creating SNMP V3 like access protection. | Supported since: V10.1.7 |
| Firewall with Black and White List | Setup a dynamic list of IP addresses that may or may not gain access to the management interface. Blacklist is combined with firewall function. | Supported since: V10.3.1 |
| TACACS+ Authentication | Users can be authenticated using central TACACS+ server. The supplied privilege levels can be mapped to any local security level. | Supported since: V10.4.0 |
| RADIUS access verification | Users that wish to gain system access may be authenticated via a RADIUS server instead of the locally stored names. Fallback to local is possible. | Supported since: V10.3.1 |

## Web Interface (WEB)

| | | |
|---|---|---|
| Base Features | Integrated Web Manager with graphical user interface (GUI) for device configuration and administration using a standard web browser. The web interface may be used to configure all aspects of the device in a convient manner.<br>Related norms: HTML v4.01,HTTP, HTTPS, Java Script | Supported since: V10.1.7 |
| Web Authentication | In order access the web interface a login/password sequence as globally defined for the device in the access section is required. | Supported since: V10.2.0 |
| RADIUS access verification | Users that wish to gain system access may be authenticalted via a RADIUS server instead of the locally stored names. Fallback to local is possible. | Supported since: V10.3.1 |
| HTTPS | HTTPS offers secure encrypted data transport. Alternative standard HTTP is also supported. When HTTPS is configured unsecure HTTP traffic is automatically blocked. | Supported since: V10.1.7 |
| Full Functional Support | All features of the device, including actions functions, are accessible from the web interface. | Supported since: V10.2.3 |
| Animated Device Graphics | When a device is selected all LED and connectors are shown as located on the device. Colored borders indicate the individual status. LEDs are showing identical to the real device. | Supported since: V10.1.7 |
| Firmware Update | Since all functions of the device are available, also firmware update is easily possible. | Supported since: V10.2.0 |
| Online Documentation | The product offers a detailed and automatically updated handbook. This handbook is readily available from the web interface. | Supported since: V10.2.0 |
| SNMP MIB download | All MICROSENS specific SNMP MIB files can be downloaded from the web interface. The MIB files are required when G6 specific functions shall be accessible via SNMP interface. | Supported since: V10.2.1 |

## Simple Network Management Protocol (SNMP)

| | | |
|---|---|---|
| SNMP V1/V2c | Simple Network Management Protocol v1, v2c (SNMPv1, v2c) to access device information stored in Management Information Base (MIB). Security provided by community strings for Set/Get commands.<br>Related norms: RFC 1155 (SMIv1), RFC 1156/1157 (SNMPv1), RFC 1901/1905/1906 (SNMPv2) | Supported since: V10.1.6 |
| SNMP V1/2c Security | SNMP v1/v2c does not provide any access protection other than an easily scanned community string. The device offers additional protection though the possibility to map SNMP requests to a certain user. Each request inherits the access rights of this user and these are applied these prior to execution. Please refer to Access section. Additionally, it is possible to generally block all SET commands. | Supported since: V10.1.7 |
| SNMP V3 | Simple Network Management Protocol v3 (SNMPv3) for secure access to device information stored in Management Information Base (MIB). SNMPv3 supports data encryption, User-based Security Model (USM) and View-based Access Control Model (VACM).<br>Related norms: RFC 3411/3412/3584 (SNMPv3), RFC 2574/ 3414 (USM), RFC 2575/3415 (VACM) | Supported since: V10.2.0 |
| Traps (SNMP V1/V2c/ V3) | Traps, Notifications or Informs can be sent to an unlimited number of independently configurable receiver destinations. Sending of message is triggered by internal device status change events. Informs provide secured messaging by requiring response message. Event triggers can be configured individually per destination. Test function to trigger Trap/ Notification for simplified configuration check | Supported since: V10.1.6 |
| Private Traps | In addition or alternatively, private traps may be generated. Any internal event that causes a syslog may also be presented as SNMP trap. This includes configuration changes or user log-in for example. There are about 80 private event types. | Supported since: V10.1.6 |
| Private and Public MIBs | The device supports private MIBS that cover every aspect of the device. Additionally numerous standard MIBs are supported. Please refer to separate documentation. Private MIB File can be downloaded from the integrated Web Manager.<br>Related norms: MIB-2, BRIDGE_MIB, Q-BRIDGE-MIB, RMON-MIB, EtherLike-MIB, POWER-ETHERNET-MIB, IGMP-STD-MIB, RADIUS-AUTH-MIB, LLDP-MIB (SMIv2), LLDP-EXT-MED-MIB, IEEE8023-DOT3-LLDP-EXT-V2-MIB | Supported since: V10.1.7 |
| ARP-Guard Compliance | Compliant with ARP-Guard (ISL GmbH) network control software which may be used for additional network security. Requires precise implementation of all BRIDGE-MIB features and other SNMP details. | Supported since: V10.3.0 |
| MACMON Compliance | Compliant with MACMON (MIKADO AG) network control software which may be used for additional network security. Requires precise implementation of all BRIDGE-MIB features and other SNMP details. | Supported since: V10.3.0 |
| Integrated SNMP Browser | SNMP commandline browser supports GET, GETNEXT, SET and WALK with all protocol levels v1/v2c/v3. Understands G6 private MIBs and some basic general purpose MIBs for easy textual retrieval. | Supported since: V10.4.1 |

## RADIUS Client

| | | |
|---|---|---|
| Access | RADIUS client via UDP/IP ports 1812 (access) for Remote Authentication Dial In User Service (RADIUS) server for authorizing user access.<br>Related norms: RFC 2865 (RADIUS), RFC 2868 (Tunnel Attributes) | Supported since: V10.2.0 |
| Accounting | RADIUS client via UDP/IP port 1813 (accounting) for Remote Authentication Dial In User Service (RADIUS) server for logging of user accounting information.<br>Related norms: RFC 2866 (Accounting) | Supported since: V10.2.0 |
| Redundancy | In case of a response timeout, a secondary RADIUS server can be requested. Up to 8 RADIUS server for use in different applications may be specified. | Supported since: V10.2.0 |

## File Management

| | | |
|---|---|---|
| File Transfer Protocols | File transfers may be used to upgrade the software or to load configuration or script files. The unit supports TFTP, FTP, SFTP, HTTP, HTTPS transfer protocols. Additionally files may be loaded via DHCP directives. The device can act as server or client for FTP, SFTP and TFTP.<br>Related norms: TFTP, FTP, SFTP, HTTP, HTTPS | Supported since: V10.1.6 |
| Firmware Download | Software download can be complete or incremental. The download is independent of its activation. Several firmware versions may reside on the SD card in parallel. | Supported since: V10.1.6 |
| Secure Firmware Update | Secure firmware update with encrypted and digitally signed upgrade files. A flexible update mechanism permits customized upgrade files if required. Configuration remains intact after firmware upgrade | Supported since: V10.3.1 |
| Firmware and Configuration Export and Import<br>*Industrial Switch only.* | Firmware update files and configuration files may be exported and re-imported by another unit via DOS formatted USB memory stick. | Supported since: V10.4.0 |
| Script Files | CLI script files may be up and downloaded in the same way as other files. This way for example a network wide special configuration can be distributed. | Supported since: V10.1.6 |
| Configuration Files | All device configurations are stored in XML files. These may be edited offline (CLI - offline mode) and then be distributed to other devices. Configuration files may be backed up to keep a save copy. A custom factory default configuration may be configured. | Supported since: V10.1.6 |
| Compare Config and create Transformation Scripts | Device configurations may be compared to view differences. Scripts file are generated that permit automated transformation of one config to another. | Supported since: V10.2.2 |

## Event Logging

| | | |
|---|---|---|
| Function | Syslog protocol for UDP/IPv4 and UDP/IPv6. Syslog messages are triggered by system events and can be sent to any number of Syslog servers.<br>Related norms: RFC 5424 | Supported since: V10.1.6 |
| Syslog to CLI | The default syslog target is the CLI. A logged-in user receives Syslogs depending on the preset severness. The filter mechanism can be tailored. | Supported since: V10.2.0 |
| Local Logfile | All events, forwarded or not, are saved to a local logfile. This permits searching to past events to aid trouble shooting. Two logfiles are used in rotation to limit the used storage. The logfile may be uploaded via file transfer. | Supported since: V10.2.0 |
| Log Filters | What is logged or forwarded as SNMP trap can be filtered independently for each log target destination. Please check Events section for details. | Supported since: V10.1.6 |

## Event Defintions

| | | |
|---|---|---|
| Event Scheme | The device internally makes extensive use of interprocess messaging. Many of these message events can be made public as Syslogs or private traps to provide insight into the internal proceedings. | Supported since: V10.1.6 |
| Customizable events | Event severeness and alert level is freely configurable for each event. Event text strings may be customized via user interface. | Supported since: V10.1.6 |
| Configuration Changes | Each time any parameter is changed via any of the user interfaces, each individual change is recorded with time stamp, operator name, user interface, old and new value. These changes may trigger Syslogs or even traps. | Supported since: V10.1.6 |
| Debug Information | It is possible to turn internal debug messages into events which can be forwarded like any other event. Thus it is possible to enable remote debugging. Note: developer/ support only. These functions are protected by customers access scheme and do not pose a security breach. | Supported since: V10.1.6 |
| Run Scripts on Event | Individual automated and programmed scripts can be attached to each event. This permits custom processes run on occurance of event. | Supported since: V10.3.1 |

## Test Functions

| | | |
|---|---|---|
| Ping, Trace Route | Use ICMP Ping test, DNS lookup and Traceroute commands. Numerous options are available. | Supported since: V10.1.6 |
| Port Mirroring | A copy of the data of a given switch port can be routed onto another (unused) port in order to connect a data monitor for trouble shooting. | Supported since: V10.3.0 |
| Test Trap | Create a test trap or Syslog to test event setup. | Supported since: V10.1.6 |
| Led Test | Turns on all LEDS in all colors to test leds. This is also useful to give attention to a specific device. | Supported since: V10.1.6 |
| ARP Cache | The ARP cache lists MAC/IP relations for Management access connections and for data streams handled by the CPU. | Supported since: V10.4.3 |

## Script Data

| | | |
|---|---|---|
| Custom Parameter | User written scripts may register individual parameter. This permits configuration of the script via any available user interface. | Supported since: V10.3.2 |
| Custom Variables | User written scripts may register individual variables to store output data of self-written scripts. This way a script may display status information. | Supported since: V10.3.2 |