Firmware Feature List

Generation 6 Ethernet Switches

Firmware Version: 10.8.3, 12.8.2, 2025-08-01

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. The G6 devices use 32bit CPU while all G8 devices and G6 HW version 2 utilize a 64bit ARM CPU.	Supported since: 10.1.0, 12.8.0
Advanced 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. Generation 6 and 8 share largely the same code base but are compiled for different microprocessors.	Supported since: 10.1.0, 12.8.0
SD Memory Card	On G6 devices all firmware and configuration is stored on an accessible memory card with microSD form factor. Certain G6 and all G8 devices use internal memory as primary memory. 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: 10.1.0, 12.8.0
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. On G8 devices internal memory is the default for firmware and configuration storage and use of the SD card is optional.	Supported since: 10.3.3, 12.8.0
Mirror SD card	A function to copy the running firmware from the SD card to internal memory of G6+ devices.	Supported since: 10.5.4, 12.8.1

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: 10.1.6, 12.8.0
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: 10.3.3, 12.8.0

System

Custom MAC address	While the MAC address is assigned at production time is possible to overwrite this MAC for special cases.	Supported since: 10.1.6, 12.8.0
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: 10.2.0, 12.8.0
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: 10.1.6, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Hardware

Function	Fanless Layer 2+ Switch controlled by high speed 1Ghz ARM CPU. The G6 devices use a 32Bit 1Ghz CPU, while the G6 Rev1.5 and all G8 devices utilize a 64Bit ARM CPU.	Supported since: 10.1.0, 12.8.0
Green IT	State-of-the-Art chip technology supports Energy Efficient Ethernet (EEE) according to IEEE 802.3az. Related norms: IEEE 802.3az	Supported since: 10.1.0, 12.8.0
Jumbo Frames	Supports Jumbo-Frames up to 10kBytes length.	Supported since: 10.1.0, 12.8.0
RGB LED	Microswitches offer full color led indicators permit extensive yet easy to remember status decoding without any tools. Quiet mode turns off most leds for unobstrusive operation. Lightshow mode helps to find a switch among others.	Supported since: 10.1.6, 12.8.0
Input / Output Pins *Industrial Switch only.*	Two decoupled input pins and two relay outputs are available in the Industry Switch. Signal changes at the input pins will trigger events (Syslog, Traps). These event 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: 10.3.0, 12.8.0
PTP Precision Time Protocol *Industrial Switch only.* *Not available with G6 device.*	The Precision Time Protocol conveys precise time information through an IP network according to IEEE 1588v2. Related norms: IEEE 1588v2	Supported since: 12.8.2

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

IP Stack

Dual Stack	Parallel handling of IPv4 and IPv6 protocol.	Supported since: 10.2.2, 12.8.0
IPv4 Stack	Internet Protocol v4 handling with support of IPv4, ARP, DHCP, ICMP. Related norms: RFC 791 (IPv4), RFC 826 (ARP), RFC 792 (ICMP), RFC 793 (TCP), RFC 768 (UDP), RFC 2131 (DHCP)	Supported since: 10.1.0, 12.8.0
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 Related norms: RFC 2131 (DHCP), RFC 2132 (DHCP Options), RFC 951 (BOOTP)	Supported since: 10.2.1, 12.8.0
Ping, Trace Route	Standard IP test functions like Ping to check reachability and trace route to visualize packet routing is available. Since 10.6.1d these are also configurable including packet size and number of pings. Related norms: RFC 792 (PING), RFC 1393 (Trace Route)	Supported since: 10.2.0, 12.8.0
IPv6 Management Access	Internet Protocol v6 handling with support of IPv6, DHCPv6, ICMPv6, NDP. IPv6 access to WEB, CLI, SNMP and NMP. 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: 10.2.2, 12.8.0
IPv6 Transport	IPv6 traffic can be transported via the switch. Filter options for enhanced security available.	Supported since: 10.2.0, 12.8.0
Dynamic ARP Inspection *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	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: 10.5.1, 12.8.1
Secondary IPv4 Address	A secondary IP address may be assigned under which the management is alternatively available.	Supported since: 10.5.4, 12.8.0
Secondary static DNS Address	A secondary DNS address may be assigned	Supported since: 10.7.9, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Ethernet Port Features

Administration	Port control. For each port a 64 character long alias name can be assigned .	Supported since: 10.1.6, 12.8.0
Ethernet Twisted-Pair	Auto-Negotiation of speed 10/100/1000, duplex mode, flow-control, Auto MDI/MDI-X Related norms: 802.3u, 802.3z	Supported since: 10.1.6, 12.8.0
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: 10.4.0, 12.8.0
Ethernet Fixed Fiber	100/1000, duplex mode, flow-control. 10G Ethernet ports in selected devices.	Supported since: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
Dual Media Ports	Some ports can operate with copper or optical cable. Preferences and priorities can be selected.	Supported since: 10.2.1, 12.8.0
Loop Protection	Local loop protection detects parallel links to the same switch or loops between local ports to avoid endless packet storms.	Supported since: 10.3.2a, 12.8.0
SFP Auto Speed	Automatically reconfigures port data rate to match the highest rate available with the plugged-in SFP. This feature requires original MICROSENS SFPs.	Supported since: 10.5.2, 12.8.0

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: 10.1.7, 12.8.0
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: 10.1.7, 12.8.0
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: 10.2.1
micro OTDR Support	Support for SFP based OTDR (optical time domain reflectometer) measurement to automatically detect changes in the fiber topology. This feature is especially suitable for the NM3 MSP1000 management module.	Supported since: 10.7.4a

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Some G8 device veriants can deliver 60W or even 90W. Related norms: 802.3af (PoE) 802.3at (PoE+)	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.2.1, 12.8.0
Emergency Port	Port can be assigned priority. Should PoE power limitation occur, the priority (emergency) port(s) are not shut down.	Supported since: 10.1.6, 12.8.0
PD Operation	PD enabled switches can be configured to operate on PoE. In this mode no other power supply is required. When one or two regular power supplies can be connected, then the PoE input can act as secondary backup supply.	Supported since: 10.3.0, 12.8.0
PoE Watchdog	PoE powered devices can be monitored by watching their data traffic or by using a PING to the device. If the device fails to respond it is restarted by briefly bringing the PoE power down and up again.	Supported since: 10.7.9a, 12.8.0

Switch / MAC

MAC Table	The device supports up to 8192 MAC addresses. MAC addresses may be learned or manually configured.	Supported since: 10.1.0, 12.8.0
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: 10.2.0, 12.8.0
SNMP Access	D-BRIDGE and Q-BRIDGE MIBs are supported. Related norms: RFC1493 (obsoletes RFC1286)	Supported since: 10.2.2, 12.8.0
MAC Limit	Limit number of allowed MAC addresses per port. Independent of other port access control functions.	Supported since: 10.5.1, 12.8.0
MAC Limit per VLAN	Limit number of allowed MAC addresses per port and VLAN. Independent of other port access control functions.	Supported since: 10.7.1, 12.8.0
Configurable MAC Aging Time	MAC aging time can be configured between 15s and 1 hour. Defaults to 5 minutes.	Supported since: 10.4.0, 12.8.0

RMON Statistics

RMON counters	35 integrated counters per port for detailed traffic analysis and network trouble shooting. 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: 10.1.7, 12.8.0
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: 10.2.3, 12.8.0
Port Mirroring	Data of one or more ports can be copied onto anohter port. On the monitoring port the data can be analyzed with an external device.	Supported since: 10.6.1, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

MSP 1000

Forward Migration	The new NM3 management module brings all the benefits of the G6 system the to the MSP1000 Optical WDM System. All features of the previous generation are retained and even legacy TeraMile and LastMile products are supported and can be upgraded.	Supported since: 10.6.0
Inventory	Automatic detection of inserted modules. Detailed inventory information are collected and presented.	Supported since: 10.6.0
Configuration and Status	All MSP 1000 modules as well as legacy TeraMile and LastMile modules can fully be configured and managed. This is possible via all management interfaces such as SNMP, Web, CLI and NMP Manager.	Supported since: 10.6.0
Alarm Correlation	In combination with NMP trap based alarms can be shown in an active list that only shows active alarm conditions. Once rectified they are removed from the alarm list.	Supported since: 10.7.4a
Active and Passive mode	In passive mode the NM3 learns the settings of all inserted modules and keeps track of them. In active mode the NM3 forces its locally defined configuration onto the other modules.	Supported since: 10.6.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

SmartOffice

General Features	SmartOffice is complete room automation system designed to measure and control office environment. This includes lighting, temperature, outlets, blinds, air condition and other facilities. Sensor and actors from MICROSENS or various third parties can be combined for a customized decentralized solutiuon. Such rooms can in turn be managed centrally from a Building Mangement System.	Supported since: 10.7.0, 12.8.0
PoE based LED Lighting	LED panels replace traditional neon tubes. The MICROSENS SmartLightController acts as an intelligent power supply that converts PoE energy to dimmable LED complatible power.	Supported since: 10.7.0, 12.8.0
Room Sensors	The MICROSENS SmartLightController includes sensors to detect ambient temperature, brightness, motion. These sensor data act as inputs to the room automation.	Supported since: 10.7.0, 12.8.0
Automatic Room	A SmartOffice can operate fully automated, based on motion and time. After a programmable idle time the room is shut down. What exactly shuts down, and what not can be configured.	Supported since: 10.7.0, 12.8.0
Configurable Graphical User Interface	A SmartOffice can also be operated very conviently via a tablet or mobile phone. The graphical user interface (GUI) is fully configurable and customizable to meet any customer requirements.	Supported since: 10.7.0, 12.8.0
Scene Based	All actions are grouped in scenes. A scene may affect every as little or as much of the parameter as desired. A scene can be global, room specific or even remotely accessed (if enabled) to be engaged from a third party.	Supported since: 10.7.0, 12.8.0
Hardware Buttons	A SmartOffice can interface to many types of physical switches. Any switch can be mapped to any scene.	Supported since: 10.7.0, 12.8.0
Scripting Language	A key feature of the SmartOffice solution is the powerful scripting engine. The script incorporates the decision logic as what to do based on sensor input. Most scripts are preinstalled during installation of the SmartDirector App, but additional custom scripts may be added to perform a wide range of features such as SNMP, HTTP or FTP operations, special office functions, etc.	Supported since: 10.7.0, 12.8.0
SmartDirector App	The SmartOffice framework offers great flexibility. In fact so much that it is sensible to offer a default functionality and graphical user interface. This interface is created by installation the SmartDirector App. For special applications, other variations of the App can be created, without affecting the general firmware of the underlying switch.	Supported since: 10.7.0, 12.8.0
microPLC	SmartOffice comes with software script controlled PLC (programmable Logic controller) function that permits PID regulators and other typical PLC applications. The microPLC does not support IEC programming but instead relies on microScript. PLC and event based operation may coexist to offer the best programming interface for any office and building automation task at hand.	Supported since: 10.7.2, 12.8.0
Remote Control Interface	A SmartOffice comes with a local graphical interface. To operate the system remotely it possible to simulate operation via an HTTPS REST API interface. When enabled, for each element indiviually, it is possile to expose a well defined set of functions, which can be controlled. Likewise,it is possible to read information from the system.	Supported since: 10.7.0, 12.8.0
enOcean support	SmartOffice support wireless automation devices using the enOcean protocol. This includes switches, relays to switch outlets, blinds and some sensors. Energy consumption monitoring is available.	Supported since: 10.7.0, 12.8.0
Homematic support	SmartOffice support wireless automation devices using the Homematic protocol. This includes switches, relays to switch outlets temperature control and other devices.	Supported since: 10.7.0, 12.8.0
Modbus/RTU support	Modbus is a standard automation bus. SmartOffice supports local serial wiring to Modbus enabled devices. Custom scripts are required for integration as there is no standard on how to interpret the data.	Supported since: 10.7.0, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Modbus/IP support	Modbus/IP is a standard automation protocol user over IP. Configurable mapping of any Modbus coil, register or memory cell to a named and data typed SmartOffice sensor or actor data point. This way Modbus devices can seamlessly be integrated into a SmartOffice installation. Related norms: IEC 61158 CPF15/1	Supported since: 10.7.2, 12.8.0
IP500 support	IP500 is an upcoming wireless automation protocol. It provides improved reliability by utilizing 866 Mhz as well as 2.4Ghz frequencies in parallel. Depending on used device, an external gateway is required which includes the required wireless hardware. Related norms: IEC 61158 CPF15/1	Supported since: 10.7.9, 12.8.0
BACnet/IP support	BACnet is an established build infrastructure interface. The device creates a BACnet server which can be read and written from other devices. The values can be linked to named and data typed SmartOffice sensor or actor data points. This way BACnet devices can seamlessly be integrated into a SmartOffice installation.We can map BACnet objects to the internal generalized database and monitor or set BACnet variables. Since such application are very installation specific, custom scripting is required for integration. Related norms: ISO 16484-5	Supported since: 10.8.3, 12.8.0
NEURON-LINK-2 support	Supports MICROSENS NEURON-LINK-2 enabled sensors with automated configuration and advanced sensing features.	Supported since: 10.8.3, 12.8.2

Controller

Smart Light Controller	Above the standard device setup in the SmartOffice section, it is possible to configure more details and features via a specific set of parameters. Support for SLC versions V2,V3 and V4.	Supported since: 10.7.1c, 12.8.0
Smart IO Controller	The Smart I/O Controller offers a host of digital and analog interfaces which need to be configured. By setting an attribute the I/O channels are linked to SmartOffice sensor and actor groups.	Supported since: 10.7.1c, 12.8.0
CSLC	The Central SmartLight Controller (CSLC) offers 24 LED ports in a single high density 1U enclosure. The G6 firmware also runs on the CSLC hardware. Support for SLC versions V2 and V4	Supported since: 10.7.7, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Virtual LANs (VLANs)

VLAN Filter	Up to 256 VLAN's may be configured. Related norms: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p	Supported since: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
Multiple VLAN Reservation Protocol (MVRP)	Multiple VLAN Reservation Protocol. This protocol automates and centralizes VLAN assignment in large networks. Related norms: IEEE 802.1ak	Supported since: 10.5.0, 12.8.0
Extreme Auto Attach (former Avaya Fabric Attach)	Support to attach to an SPB based network by mapping local VLANs to SPB I-SIDs. SPB is the basis of the Avaya Fabric, now Extreme.	Supported since: 10.6.1, 12.8.0
Extreme (Avaya) Zero Touch	Attach to an SPB based network,automatically obtaining the VLANs - I-SID bindings over the network. Note: Requires preset of authentication key to match network.	Supported since: 10.7.5, 12.8.0
Stacked VLANs (Q-in-Q)	Stacked VLAN are used to transport customer VLAN traffic accross a carrier network using VLAN itself. The feature is also known as Q-in-Q and provider bridging. Configurable Ethertype fields are provided. Related norms: IEEE 802.1ad	Supported since: 10.7.0, 12.8.0
Priority Override	VLAN priority code point of incoming packets can be overwritten with the VLAN specific priority defined in the VLAN filter.	Supported since: 10.1.7, 12.8.0
Voice VLAN	VLAN ID used by LLDP/CDP to assign VLAN to connected VoIP-phone.	Supported since: 10.1.7, 12.8.0
RSTP VLAN	VLAN ID used by Spanning Tree instance for BPDU tagging.	Supported since: 10.1.7, 12.8.0
Unauthorized VLAN	VLAN ID assigned by Port Based Access Control to unauthorized ports (guest VLAN).	Supported since: 10.1.7, 12.8.0
Management VLAN	VLAN ID used by the management agent (device internal port).	Supported since: 10.1.7, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Quality of Service (QoS)

Priority Queues	4 priority queues per port.	Supported since: 10.1.6, 12.8.0
Prioritization Scheme	Strict priority (higher priority always first) or weighted fair queuing (8:4:2:1 highest to lowest).	Supported since: 10.1.6, 12.8.0
Layer1 Priority	Static priority queue can be assigned for each port.	Supported since: 10.1.6, 12.8.0
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. Related norms: IEEE 802.1p (VLAN priority code point)	Supported since: 10.1.6, 12.8.0
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. Related norms: RFC 2474/3260 (IPv4 DiffServ/IPv6 Traffic Class)	Supported since: 10.1.6, 12.8.0
Egress Rate Shaping	Egress rate shaping may be used to limit the data traffic coming out of a port. (bandwidth limitation)	Supported since: 10.5.0, 12.8.0
Ingress Rate Shaping	Ingress rate shaping may be used to limit the amount of data traffic an access port can accept. (bandwidth limitation)	Supported since: 10.6.1, 12.8.0

Spanning Tree Protocols

Spanning Tree (STP)	Automatic detection of loops and redundant network paths. Single STP instance running in configurable VLAN.	Supported since: 10.2.0, 12.8.0
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. Related norms: IEEE 802.1D-1998 IEEE 802.1D-2004 IEEE 802.1w	Supported since: 10.2.0, 12.8.0
Multiple Spanning Tree (MSTP)	Up to 64 STP instances running in configurable VLAN groups. Related norms: IEEE 802.1s IEEE 802.1Q	Supported since: 10.3.2a, 12.8.0
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: 10.3.0, 12.8.0
Bridge Assurance	Detects unidirectional link failures that may occur with fiber optic links whereby one fiber direction breaks.	Supported since: 10.3.2a, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Port Access Control

IEEE 802.1X Authentication	Multiple users can be authenticated using central RADIUS server based on username/password or certificate. 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,EAP-FAST	Supported since: 10.2.1, 12.8.0
IEEE 802.1X Supplicant *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	An IEEE 802.1X Supplicant can authenticate the device at the port access controlled uplink port. Username/password and certificate based methods are supported (EAP-MD5, PEAP). Related norms: EAP-MD5, PEAP	Supported since: 10.7.0, 12.8.0
RADIUS MAC Authentication	Multiple users can be authenticated using central RADIUS server based on their MAC addresses. Related norms: EAPOL, RADIUS	Supported since: 10.2.1, 12.8.0
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: 10.2.1, 12.8.0
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: 10.2.1, 12.8.0
Limited number of MACs	A port may be limited to accept only a configurable number of MACs on a given port (1 - 255). Additional MACs are blocked in the hardware layer.	Supported since: 10.5.1, 12.8.0
Limited number of MACs per VLAN	A port may be limited to accept only a configurable number of MACs on a given port (1 - 255) and VLAN..	Supported since: 10.7.0, 12.8.0
Learned MAC time out	Time out of learned MACs to allow another computer to connect in MAC locking environment.	Supported since: 10.4.0, 12.8.0
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: 10.2.1, 12.8.0
Allowed Outgoing Port (Port based VLANs)	This feature is used to limit the outgoing traffic for each port to certain destination ports. This feature is also known as port based VLAN.	Supported since: 10.7.0, 12.8.0
IP Address Logging	The IP address of the connected user is detected via ARP snooping. User IP address information can be logged locally and using RADIUS accounting function.	Supported since: 10.5.1, 12.8.0
Wake-on-Lan support	A solution to send out Wake-on-LAN packets on a PACC blocked port. This feature is also called Unidirectional Controlled Port or Admin Controlled Directions in the IEEE 802.1X-2004 specification.	Supported since: 10.6.1d, 12.8.0
Network Edge Authentication	The network edge authentication mode is used to authenticate a "supplicant switch" connected to a downlink port of the switch. After successful authentication the port should be open for any traffic from the downstream switch. Similar to Cisco NEAT feature.	Supported since: 10.7.0, 12.8.0
Authentication Fail Retry Timer	When authentication has failed, the authentication is restarted after the defined time in seconds.	Supported since: 10.7.0d, 12.8.0
Change of Authorization	The feature CoA permits un-authorization followed by a re-authentication of a running session initiated from an Authentication Server via RADIUS protocol. Related norms: RFC 3576 (CoA)	Supported since: 10.7.9, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Related norms: RFC 4541 (IGMP)	Supported since: 10.2.0, 12.8.0
IGMP Snooping per VLAN	Automatic detection and forwarding of IPv4 multicast-streams independent for each configured VLAN.	Supported since: 10.3.0, 12.8.0
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. Related norms: RFC 3810/4604 (MLD), RFC4541	Supported since: 10.3.2a, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

DHCP

DHCP Snooping *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	DHCP snooping records IP addresses, VLAN information, etc. to record trusted interfaces. DHCP snooping supresses DHCP traffic from untrusted interfaces.	Supported since: 10.5.1, 12.8.0
IP-MAC Binding Table *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	A table lists the MAC-IP bindings of the untrusted ports (only) as discovered through DHCP snooping.	Supported since: 10.5.1, 12.8.0
DHCP Filtering *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	DHCP Filtering prevents DHCP being injected from a user port. This feature acts on IPv4 and IPv6 alike.	Supported since: 10.5.0, 12.8.0
DHCP Flooding Detection *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	Attempts to detect a DHCP attack and shuts down the access port when too many DHCP messages ingress on the port.	Supported since: 10.5.0, 12.8.0
DHCP relay agent with option 82	When enabled, the switch will append a unique port/switch identification to a DHCP request from an access port. This enables the use of a distant DHCP server and to better control which IP address to serve. This feature supports IPv4 and IPv6. Port and unit information are configurable.	Supported since: 10.5.1, 12.8.0
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 Related norms: RFC 2131 (DHCP)	Supported since: 10.2.1, 12.8.0
Dynamic ARP Inspection *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	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: 10.5.1, 12.8.0
PPPoE Snooping	PPP over Ethernet is used by carriers to identify the customer port. When a user signs-in, The Switch will automatically insert a configurable information that will allow the network to identifiy the originating port and device. Related norms: RFC 2516	Supported since: 10.7.0, 12.8.0
PPPoE variable Remote and Circuit Ids	PPP over Ethernet is used by carriers to identify the customer port. The fields for remote-id and circuit-id can be configured in various ways to match network requirements. Related norms: RFC 2516	Supported since: 10.7.0d, 12.8.0
RADIUS controlled dynamic IP-Address provisioning with DHCP	This function applies the IP configuration by DHCP to a successful authorized host. The IP parameters are received from the RADIUS server when granting network access to the host.	Supported since: 10.7.6, 12.8.0
DHCP Server	When enabled, this function provides an IP address to other computers. The address range and lease time is configurable.	Supported since: 10.7.9, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Related norms: RFC 4330 (SNTP)	Supported since: 10.1.7, 12.8.0
NTP Server	This may be used in an island network where other devices cannot reach outside. The quality of the local ntp server depends on how the local time is sourced and maintained. Related norms: RFC 4330 (SNTP)	Supported since: 10.8.2, 12.8.2

Redundant Ring Protocol

MICROSENS Ring Protocol	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. The previous generation G5 and the G6 Ring protocols are compatible and interwork.	Supported since: 10.4.1
Media Rundancy Protocol (MRP) *Industrial Switch only.*	MRP is an alternative ring redudancy protocol. It is predominatly used in ProfiNet networks. Related norms: Redundanz Manager	Supported since: 10.8.3, 12.8.2
Ethernet Ring Protection Switching (ERPS) *Industrial Switch only.*	ITU-T G.8032 Ethernet Ring Protection Switching is an alternative ring protocol supported by various vendors. Related norms: ITU-T G.8032	Supported since: 10.8.3, 12.8.2

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. Related norms: IEEE 802.1AB (LLDP)	Supported since: 10.2.1, 12.8.0
LLDP transmission	Geographical coordinates and civic location information can be specified for transmission to neighboring devices.	Supported since: 10.2.1, 12.8.0
LLDP-MED	Media Endpoint Discovery for the auto-discovery of LAN policies. Support of VLAN advertising and PoE+ control. Related norms: ANSI/TIA-1057 (LLDP-MED)	Supported since: 10.2.2, 12.8.0
LLDP/CDP preference	Device will prefer standards based LLDP but will automatically accept CDP if present.	Supported since: 10.2.0, 12.8.0
CDP operation	Support for Cisco Discovery Protocol CDP v1, v2 for automatic detection of capabilities of neighbor CDP enabled devices.	Supported since: 10.2.0, 12.8.0
CDP Voice VLAN	Support of Voice VLAN for configuration of connected Cisco VoIP-phone.	Supported since: 10.2.0, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Link Aggregation Control Protocol (LACP)

Static Link Aggregation	Multiplies available bandwidth between two end points. The setup is manually. Up to 16 groups of any number of ports per group. Related norms: IEEE 802.1ax, IEEE 802.3ad	Supported since: 10.3.2a, 12.8.0
Dynamic Link Aggregation	Multiplies available bandwidth between two end points. The setup is dynamic within a predefined group of ports. Related norms: IEEE 802.1ax, IEEE 802.3ad	Supported since: 10.3.2a, 12.8.0
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: 10.3.2a, 12.8.0
IEEE 802.1X Supplicant should authenticate on every port of a LACP trunk	If the uplink interface of the device is an aggregated LACP trunk, it is possible to use the IEEE 802.1X Supplicant to authenticate on the upstream switch port. To use this feature just configure the Supplicant port as one of the ports of the LACP trunk.	Supported since: 10.7.6, 12.8.0

Access Control Lists (ACL)

Access Control Lists (ACL) *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	ACL permit comprehensive wirespeed filtering of incoming data. This advanced feature may be used to block malicious or unwanted data from entering the network.	Supported since: 10.6.1, 12.8.0
Dynamic ACL via RADIUS *Not available with hardware 1.5 / Only available on ports [2/*] with hardware 1.6.*	Dynamic ACL ease deployment of ACL settings by centralizing their setup. The ACL setting are received during 802.1X port authentication and are automatically applied.	Supported since: 10.7.1, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

IoT Protocol MQTT

Auto publish actor, sensor and GUI data	Any changes to sensor or actor data of the entire SmartOffice system can automatically be published. Likewise, any GUI activity can be published. Features can be enabled individually. Related norms: MQTT V3.1.1	Supported since: 10.7.1c, 12.8.0
Auto subscribe actor, sensor and GUI data	Any sensor or actor data of the entire SmartOffice system can automatically be accessed. Likewise, the GUI can be remote controlled. Features can be enabled individually. Related norms: MQTT V3.1.1	Supported since: 10.7.4, 12.8.0
Topic Map	MQTT data from other systems can be subscribed to and are automatically mapped to local SmartOffice sensors. Similarly, individual actor group changes can be published to control remote devices.	Supported since: 10.7.1c, 12.8.0
Configuration via MQTT	MQTT may be used to access any configuration parameter. Read and write access is supported. For security the feature canbe switched off or limited to read only. In addition user access rights of command level can be applied.	Supported since: 10.7.7, 12.8.0
Script Execution via MQTT	MicroScripts that already reside on the system can be executed via MQTT. Topic payload and extra topic elements are forwarded to the Script as parameters. The permitted scripts can precisely be defined.	Supported since: 10.7.7, 12.8.0
Local broker	Typically, a third party broker is accessed to transfer information. When such a broker is not available, a local broker can be provided.	Supported since: 10.7.1c, 12.8.0
Encrypted broker	For security encryption broker connection are used featuring SSL with custom certificates etc.	Supported since: 10.8.2, 12.8.2
Data Transformation	Often data are not available in a compatible format among several devices of different vendors. Transformation rules permit on-the-fly transformation and calculations to achieve uniform data representation.	Supported since: 10.7.2, 12.8.0
Retain Flag	When a message it sent marked as retained then it is saved by the broker and retured to a new client upon connect, even if the originating device is not sending it again.	Supported since: 10.8.2, 12.8.2

Automation Protocol Modbus

Element Map	Modbus data from other systems can be read and are mapped to local SmartOffice sensors. Similarly, individual actor group changes can be written to a Modbus device.	Supported since: 10.7.2, 12.8.0
Data Formatting	Modbus data come raw with no indication of meaning and purpose. With formatting applied, the data can be converted to numbers, strings or floating point values that are easily understood.	Supported since: 10.7.2, 12.8.0
Data Transformation	Often data are not available in a compatible format among several devices of different vendors. Transformation rules permit on-the-fly transformation and calculations to achieve uniform data representation.	Supported since: 10.7.2, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Automation Protocol BACnet/IP

Element Map	BACnet data types BINARY and ANALOG can be created and mapped to local SmartOffice elements. BACnet data may directly cause script handling or read/write sensor or actor groups. Related norms: ISO 16484-5	Supported since: 10.8.3, 12.8.2
BACnet test functions	The BACnet whois and whohas functions are available. In addition BACnet values on any server can directly be read and written via console commands, mainly for testing. A BACnet trace mode is also available.	Supported since: 10.8.3, 12.8.2
Data Transformation	Often data are not available in a compatible format among several devices of different vendors. Transformation rules permit on-the-fly transformation and calculations to achieve uniform data representation.	Supported since: 10.8.3, 12.8.2

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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: 10.1.6, 12.8.0
Context Sensitive Help	Type ? anywhere while editing and context sensitive help regarding the current parameter is provided.	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.7, 12.8.0
microScript Language	Powerful and comprehensive script language permits customized active functions which greatly increase flexibility of the product.	Supported since: 10.3.1, 12.8.0
Timer Controlled Scripting	Scripts support timed single shot or cyclical invocation. Useful to implement time outs for error handling,	Supported since: 10.6.1, 12.8.0
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: 10.2.1, 12.8.0
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: 10.4.1, 12.8.0
Create Snapshot	Creates a snapshot of all relevant system information inluding all config, status, internal process details.	Supported since: 10.4.1, 12.8.0
Live Syslog	Syslog events can be forwarded to the active console the moment they occur. Filtering according to logging setup applies. Related norms: RFC3164	Supported since: 10.2.0, 12.8.0
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. Related norms: RFC 854 (Telnet) via TCP/IP port 23.	Supported since: 10.1.7, 12.8.0
Secure Shell (SSH)	An SSH session automatically invokes the cli. SSH may be disabled by configuration. Related norms: SSH via TCP/IP port 22. Authentication methods: RSA, Diffie-Hellman Key Exchange. Encryption protocols: 3DES-CBC, HMAC-SHA1.	Supported since: 10.1.6, 12.8.0
SSH CLI-Commands	It is possible to supply any CLI command directly in the SSH connect. The CLI command is executed and the connection is dropped immediately.	Supported since: 10.7.9a, 12.8.0
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: 10.3.2a, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Umlaut Support	Support for German Umlaute, French Accents, etc. in all user interfaces for selected parameters. Supports ISO 8859-1 coding.	Supported since: 10.4.1, 12.8.0
Favorites	Most often used commands can be entered as favorites and then be executed with a single key stroke (F). Related norms: RFC 854 (Telnet) via TCP/IP port 23.	Supported since: 10.6.0, 12.8.0

Login Access Protection

Unlimited number of Users	Three default users are created and any number of additional users may be created.	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
General access rights	For quick and effective rights management the general read/ write privileges of a user can be selected.	Supported since: 10.1.6, 12.8.0
Disable Insecure Interfaces	It is possible to restrict management access to secure interfaces such as HTTPS, SSH, SNMP V3	Supported since: 10.1.6, 12.8.0
Interface Restrictions	For each user the permitted user interfaces can be selected.	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.7, 12.8.0
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: 10.3.1, 12.8.0
TACACS+ Authentication	Users can be authenticated using central TACACS+ server. The supplied privilege levels can be mapped to any local security level.	Supported since: 10.4.0, 12.8.0
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: 10.3.1, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Related norms: HTML v4.01,HTTP, HTTPS, Java Script	Supported since: 10.1.7, 12.8.0
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: 10.2.0, 12.8.0
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: 10.3.1, 12.8.0
HTTPS	HTTPS offers secure encrypted data transport. Alternative standard HTTP is also supported. When HTTPS is configured unsecure HTTP traffic is automatically blocked. Since 10.7.7 only TLS 1.2 is supported. For older TLS versions a new parameter setting (LESS_SECURE) was added. Related norms: TLS1.2	Supported since: 10.1.7, 12.8.0
Less Secure HTTPS	Since 10.7.7 the less secure standards TSL1.0 and TSL1.1 as well as SSLv2 and SSLv3 are no longer supported when HTTPS is selected. The less secure setting for HTTPS makes these older standard available if required. Related norms: TSL1.0, TSL1.1, SSLv2, SSLv3	Supported since: 10.7.7, 12.8.0
Custom SSL Certificates	Custom SSL certificate for secure web access can be up and downloaded via file transfer. Also chain files are supported.	Supported since: 10.5.1, 12.8.0
Full Functional Support	All features of the device, including actions functions, are accessible from the web interface.	Supported since: 10.2.3, 12.8.0
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: 10.1.7, 12.8.0
Firmware Update	Since all functions of the device are available, also firmware update is easily possible.	Supported since: 10.2.0, 12.8.0
Online Documentation	The product offers a detailed and automatically updated handbook. This handbook is readily available from the web interface.	Supported since: 10.2.0, 12.8.0
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: 10.2.1, 12.8.0
Event Display	the 20 latest events (traps) are visible in the web interface for immediate detection of special conditions. An individual log filter may be set.	Supported since: 10.7.2, 12.8.0
REST API interface	All configuration, status and SmartOffice parameter can be accessed remotely using an REST interface. Versions with and without JSON are available. Multiple objects can be processed per message. All access protection schemes apply. SSH is used.	Supported since: 10.7.4, 12.8.0
Configurable Web GUI	In addition to the normal Web interface, an additonal fully configurable interface exist which can be used to provide custom GUI for SmartOffice and other applications.	Supported since: 10.7.0, 12.8.0
Responsive Web GUI	The configurable Web GUI has been further enhanced to support PC and Mobile devices and in any orientation with adapting screen elements.	Supported since: 10.7.9a, 12.8.0
Web GUI Styles	The configurable Web GUI supports style templates which can fully alter the appearance including color, background images and fonts.	Supported since: 10.7.9a, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Related norms: RFC 1155 (SMIv1), RFC 1156/1157 (SNMPv1), RFC 1901/1905/1906 (SNMPv2)	Supported since: 10.1.6, 12.8.0
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: 10.1.7, 12.8.0
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). Related norms: RFC 3411/3412/3584 (SNMPv3), RFC 2574/3414 (USM), RFC 2575/3415 (VACM)	Supported since: 10.2.0, 12.8.0
SNMP TSM	Support of Transport Security Model TSM for SNMP v3. This includes agent und user certificates . SNMP traffic is tunnelled via SSH. Related norms: RFC 5591/5592	Supported since: 10.7.4, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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. 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: 10.1.7, 12.8.0
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: 10.5.4c, 12.8.0
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: 10.3.0, 12.8.0
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: 10.4.1, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

RADIUS Client

Access	RADIUS client via UDP/IP ports 1812 (access) for Remote Authentication Dial In User Service (RADIUS) server for authorizing user access. Related norms: RFC 2865 (RADIUS), RFC 2868 (Tunnel Attributes)	Supported since: 10.2.0, 12.8.0
Accounting	RADIUS client via UDP/IP port 1813 (accounting) for Remote Authentication Dial In User Service (RADIUS) server for logging of user accounting information. Related norms: RFC 2866 (Accounting)	Supported since: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
Tunnel Attributes	When port-based network access control and VLANs are enabled additional RADIUS attributes can be added to the RADIUS ACCESS-REQUEST frames. Related norms: RFC 3580, RFC2868	Supported since: 10.7.0a, 12.8.0

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, FTPS and TFTP. Related norms: TFTP, FTP, SFTP, HTTP, HTTPS	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.3.1, 12.8.0
Firmware and Configuration Export and Import *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: 10.4.0, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.2.2, 12.8.0
Temporary Configuration	Usually, the device configuration should be saved permanently. For some applications like public kiosk systems it is desireable to only temporarily activate a configuration and start afresh with the next user.	Supported since: 10.7.0a, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

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. Related norms: RFC 5424, RFC 3164	Supported since: 10.1.6, 12.8.0
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: 10.2.0, 12.8.0
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: 10.2.0, 12.8.0
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: 10.1.6, 12.8.0
Recent Logs	The recent logs table hold the last 15 events in reverse order. The lastets event at the top. This can be used in combination or instead of the instant event display in the CLI.	Supported since: 10.7.0, 12.8.0
Log to MQTT topic	Event messages can be forwarded as MQTT topics. Different format options apply. A fixed or a dynamic topic can be selected.	Supported since: 10.7.5, 12.8.0
Long Term History	Up to 15 arbitrary status parameter can be defined which will internally be sampled every second. The values are then accumulated the last minute, hour and day. In addition logfiles are written which permit backtracking the data monthly. The created csv files can be forwarded to a collection server for further processing in Excel or similar tools.	Supported since: 10.7.0, 12.8.0

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: 10.1.6, 12.8.0
Customizable events	Event severeness and alert level is freely configurable for each event. Event text strings may be customized via user interface.	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
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: 10.3.1, 12.8.0

©2024 MICROSENS GmbH & Co. KG - Küferstraße 16, D-59067 Hamm/Germany - www.microsens.com

Test Functions

Ping, Trace Route	Use ICMP Ping test, DNS lookup and Traceroute commands. Numerous options are available.	Supported since: 10.1.6, 12.8.0
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: 10.3.0, 12.8.0
Test Trap	Create a test trap or Syslog to test event setup.	Supported since: 10.1.6, 12.8.0
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: 10.1.6, 12.8.0
ARP Cache	The ARP cache lists MAC/IP relations for Management access connections and for data streams handled by the CPU.	Supported since: 10.4.3, 12.8.0

Script Data

Custom Parameter	User written scripts may register individual parameter. This permits configuration of the script via any available user interface.	Supported since: 10.3.2a, 12.8.0
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. Alternatively use persistent variables.	Supported since: 10.3.2a, 12.8.0

Misc

Terminal Server	The serial port can be used to connect a foreign device. This device can than be reached via Telnet or SSH session. Also serial to serial connections via an IP network are supported. The serial port can also be reached via a PC-COM port emulation.	Supported since: 10.6.0, 12.8.0
Loudspeaker support	Audio files (wav, mp3) and network audio streams can be streamed to external IP loudspeaker. Play function can be scripted and associated to selected events.	Supported since: 10.6.0, 12.8.0

This document in whole or in part may not be duplicated, reproduced, stored or retransmitted without prior written permission of MICROSENS GmbH & Co. KG. All information in this document is provided 'as is' and subject to change without notice. MICROSENS GmbH & Co. KG disclaims any liability for the correctness, completeness or quality of the information provided, fitness for a particular purpose or consecutive damage. A product feature listed in this document is not part of a sales contract between the final customers and vendors, if the specific product feature was released after the effective date of the corresponding sales contract. Each feature description listed above includes: release schedule and version number. MICROSENS is a trademark of MICROSENS GmbH & Co. KG. Any product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.